JUN 14 2005
PATENT & TRADEMARK OFFICE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	
Edward Rodriquez et al.	Group Art Unit: 3623
Application No.: 09/811,823	Examiner: Akiba K Robinson Boyce
Filed: March 20, 2001	Confirmation No.: 9310
For: METHOD AND SYSTEM FOR ELECTRONIC VOTER REGISTRATION AND ELECTRONIC VOTING OVER A NETWORK	

DECLARATION UNDER 37 C.F.R. § 1.131

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

We, Edward Rodriguez, Thomas K. Vander Vlis and Peter J. Butziger declare that:

1. We are the inventors of the subject matter disclosed and claimed in the above-referenced patent application.

2. We are familiar with U.S. Patent Application Publication No. US 2002/0133396 A1 (the '396 Application), filed March 13, 2001 and published September 19, 2002 (attached hereto as **Exhibit A**). The present application was filed March 20, 2001, one week after the '396 Application was filed. However, the present application was conceived and reduced to practice well before the filing date of the '396 Application as evidenced herein. Because no statutory bar exists regarding the '396 Application, this Declaration is appropriate under 37 C.F.R. § 1.131.

BEST AVAILABLE COPY

3. The presently claimed invention was reduced to practice prior to the March 30, 2001 filing date of the '396 Application. Documents submitted herewith have been redacted to remove date information. However, the documents establish that conception, and actual reduction to practice, of the presently claimed invention occurred at a time before the national election in November of 2000.

4. A 37 page document prepared prior to November 2000, entitled "Security in the System", is attached as **Exhibit B**, and has been redacted to remove date and some non-relevant information. The pages of this document were not numbered in their original form. Numbers have been added in the lower right hand corner of each page for ease of referencing them in this Declaration. This **Exhibit B** document details features of the presently claimed invention as having been reduced to practice well before the March 30, 2001 filing date of the '396 Application.

5. The **Exhibit B** document shows, on the third page, a method and system as illustrated in Figure 1 of the present application.

6. A 51 page document prepared prior to November 2000, entitled "System Overview" is attached as **Exhibit C**, and has been redacted to remove date and some non-relevant information. Page 5 of **Exhibit C** corresponds to Fig. 1 of the present application. Although the subject matter illustrated in Figs. 6A-6C of the present application is supported by **Exhibit B**, the **Exhibit C** document shows on pages numbered 6 through 8, systems and methods which closely correspond to Figs. 6A-6C of the present application.

7. The **Exhibit B** document shows, for example, on page 9, functional steps which correspond to an exemplary embodiment of the claim 1 feature for transmitting a blank electronic registration form, upon request at a first computer, via a transaction mediator, to the first computer for retrieval by a citizen at the first computer. Pages 10-13 of **Exhibit B** show functional steps which correspond to an exemplary embodiment for the claim 1 feature of transmitting registration information from a first computer, via the transaction mediator, to a computer database that

resides on a transaction repository server, all of which are networked together, to establish a registered voter. **Exhibit B** shows, for example, on page 17, functional steps which correspond to an exemplary embodiment of the claim 1 feature for transmitting a blank electronic ballot, upon request by the registered voter at a second computer, from the computer database that resides on the transaction repository server, via the transaction mediator, to the second computer. Pages 18-21 of **Exhibit B** show functional steps which correspond to an exemplary embodiment of the claim 1 feature for transmitting a voted electronic ballot from the second computer, via the transaction mediator, to the computer database that resides on the transaction repository server. Similar features are recited in claims 23-26, 32-35 and 41-43.

8. **Exhibit B** shows, for example, on pages 26-28, use of an encrypted communication channel which corresponds to an exemplary embodiment of the features recited in claims 4 and 44. **Exhibit B**, page 10, shows steps which correspond to exemplary embodiment of the registration information feature recited in claims 5 and 45. **Exhibit B**, page 10, shows functional steps which correspond to an exemplary embodiment of the entry of registration information, and a digital signing information using a signature and public key infrastructure (PKI) of page 3, which inherently uses an asymmetric cryptographic function as recited in claims 6, 27 and 36. **Exhibit B**, page 12, shows functional steps which correspond to an exemplary embodiment of the verifying features recited in claim 8. **Exhibit B**, pages 10-18, illustrates additional functional steps which correspond to the exemplary embodiment of the features recited in claims 9, 28 and 37, with respect to the public key infrastructure. **Exhibit B**, pages 16-18, shows functional steps which correspond to an exemplary embodiment for performing the features of claims 12, 29 and 38 with respect to digitally signing a blank electronic form using the public key infrastructure. **Exhibit B**, page 18, shows functional steps which correspond to an exemplary embodiment of the features recited in claims 13, 30 and 39 for executing a blank electronic ballot, encrypting a voting electronic ballot, encrypting the key and digitally signing an encrypted voting electronic ballot. **Exhibit B**, page 20, shows functional steps which correspond to an exemplary embodiment of the verifying

features recited in claim 15. **Exhibit B**, pages 22-23,shows functional steps which correspond to an exemplary embodiment of reconciling transmitted voted electronic ballots as recited in claim 16.

9. **Exhibit C** shows, for example, on pages 44-45 functional steps which correspond to exemplary embodiment of the features recited in claims 2, 20-21 and 46 regarding the establishment of a computer database on a transaction repository server that contains information associated with one of a voter registration status of a citizen and an electronic ballot status, in conjunction with steps of requesting, determining and transmitting as recited in claims 2 and 20. **Exhibit C**, page 45, shows functional steps which correspond to an exemplary embodiment of the claim 3 feature regarding verification of voter registration status and electronic ballot status as recited in claims 3, 22 and 27. **Exhibit C**, page 30, shows functional steps which correspond to exemplary embodiments of the claim 10 feature for approving or denying a registration request.

10. A two page document (**Exhibit D**) prepared subsequent to March 30, 2001, entitled "Project Assessment Report", is further evidence of an actual reduction to practice prior to the November 2000 election, and thus prior to the March 30, 2001 filing date of the '396 Application. The second page of this document is a letter from a customer of the assignee, Booz-Allen & Hamilton, of the present application. The letter recognizes the development team, including inventors of the presently claimed invention, for their efforts in ensuring that the "System" was fielded on schedule by November 2000. The "System" referred to in this letter is an embodiment of the system described and illustrated in **Exhibit B** and in **Exhibit C**. The reference in this letter to the "System" having been "fielded on schedule" refers to a successful reduction to practice of an embodiment of the presently claimed invention prior to November 2000, and thus prior to the March 13, 2001 filing date of the '396 Application.

11. We hereby declare that all statements made herein of our own knowledge are true and that all statements made upon information and belief are believed to be

true; and further that these statements and the like so made are punishable by fine or imprisonment, or both, under 18 United States Code section 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Date: 6/14/05 Edward Rodriguez

Date: 6/14/05 Thomas K. Vander Vlis

Thomas K. Vander Vlis

Date: 6/14/05 Peter J. Butziger

Peter J. Butziger

EXHIBIT A

U.S. Patent Application Publication No. US 2002/0133396 A1 filed March 13, 2001 and published September 19, 2002

US 20020133396A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2002/0133396 A1

Barnhart (43) Pub. Date: Sep. 19, 2002

(54) METHOD AND SYSTEM FOR SECURING NETWORK-BASED ELECTRONIC VOTING

(76) Inventor: Robert M. Barnhart, San Diego, CA (US)

Correspondence Address:
KILPATRICK STOCKTON LLP
607 14TH STREET, N.W.
SUITE 900
WASHINGTON, DC 20005 (US)

(21) Appl. No.: 09/805,279

(22) Filed: Mar. 13, 2001

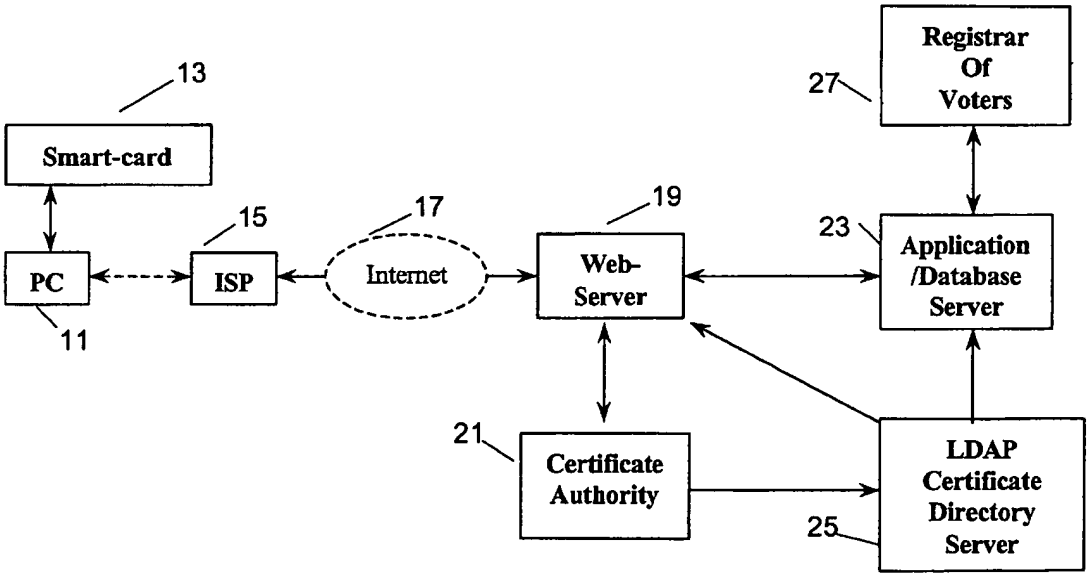
Publication Classification

(51) Int. Cl.[7] G06F 17/60

(52) U.S. Cl. 705/12

(57) ABSTRACT

A method and system for securely voting over a network, such as a global computer network, involves a system which delivers an electronic ballot from a server with the server's private key and a vote serial number on the ballot to an individual terminal connected to the network. The ballot may be filled in and a subset of the filled-in ballot is created with a digital signature created from the individual's secret key on the subset of the ballot corresponding to the ballot choices. The subset of the filled-in ballot together with the individual's electronic signature, and a vote serial number is then delivered to the server. A data element is then created to record a subset of the ballot in a data store at the server, in which the ballot vote information is retained as a vote.



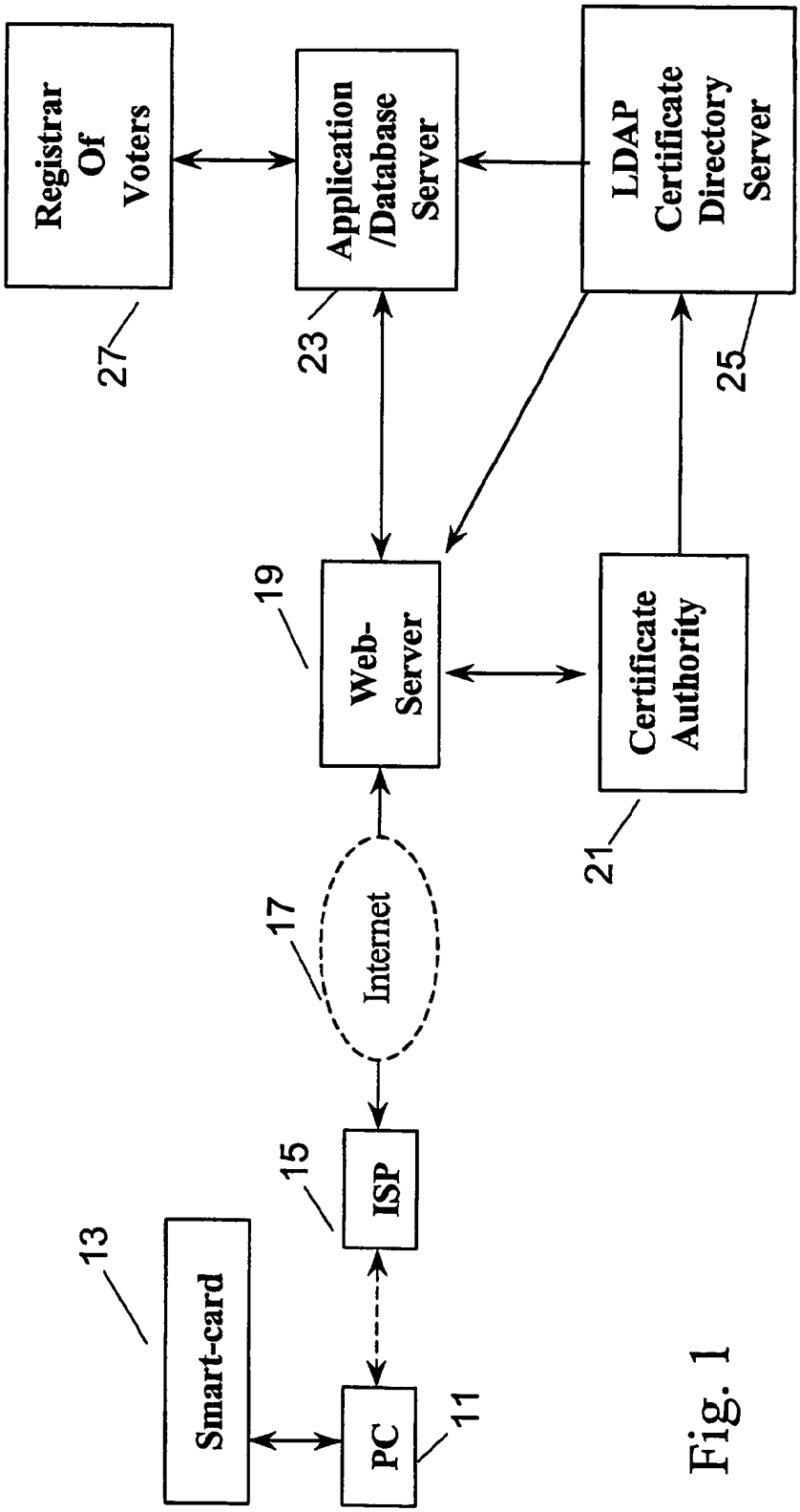

Registrar Of Voters
Application /Database Server
LDAP Certificate Directory Server
27
23
25
19
Web-Server
Certificate Authority
21
17
Internet
15
ISP
13
Smart-card
PC
11

Fig. 1

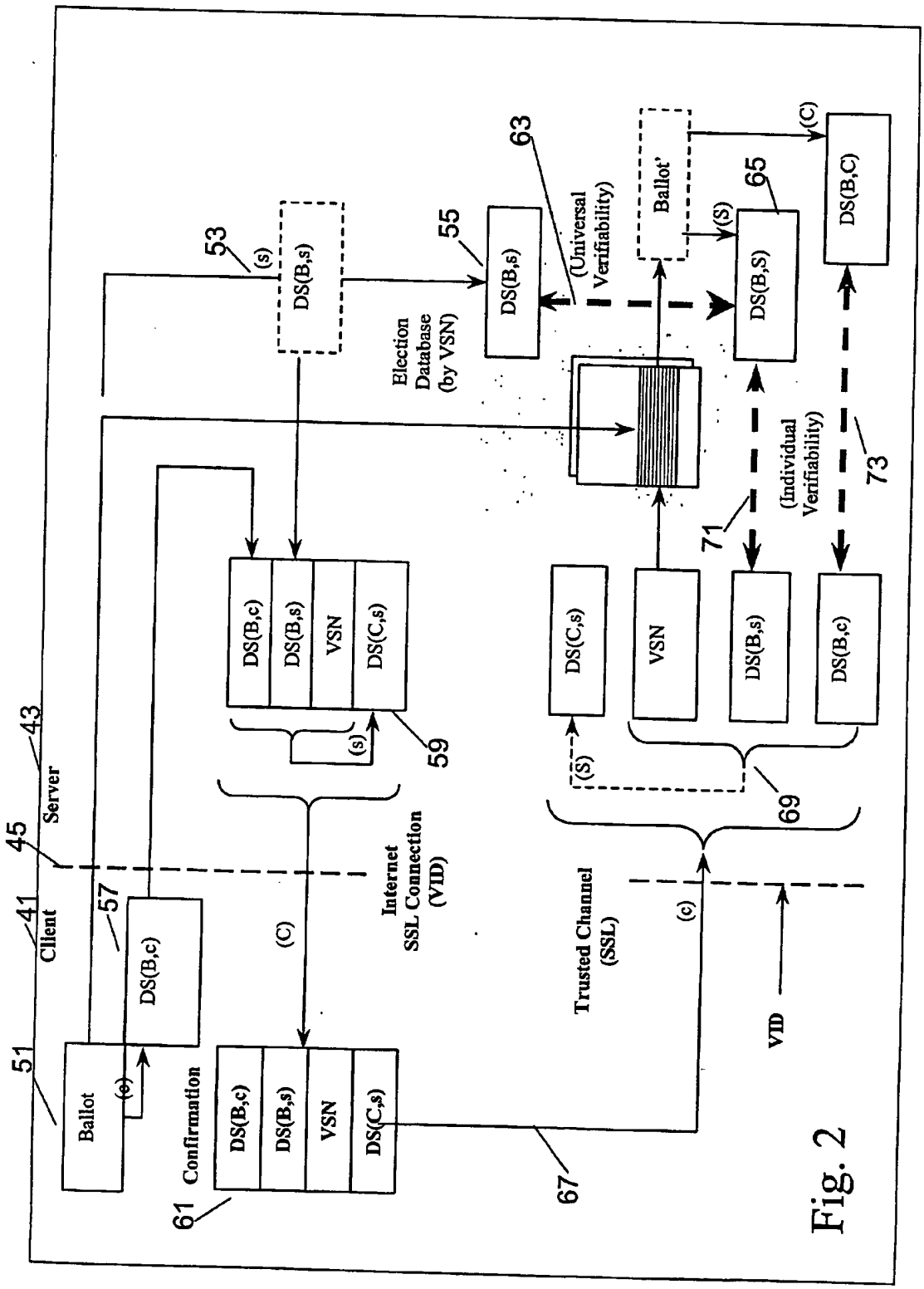

Server
43
45
Client
41
57
DS(B,c)
Ballot
51
(e)
Confirmation
DS(B,c)
DS(B,s)
VSN
DS(C,s)
61
(C)
Internet
SSL Connection
(VID)
DS(B,c)
DS(B,s)
VSN
DS(C,s)
(s)
59
53
(s)
DS(B,s)
Election
Database
(by VSN)
55
DS(B,s)
63
(Universal
Verifiability)
Ballot'
(S)
65
DS(B,S)
(C)
DS(B,C)
71
(Individual
Verifiability)
73
DS(C,s)
VSN
DS(B,s)
DS(B,c)
(S)
69
Trusted Channel
(SSL)
(c)
VID
67

Fig. 2

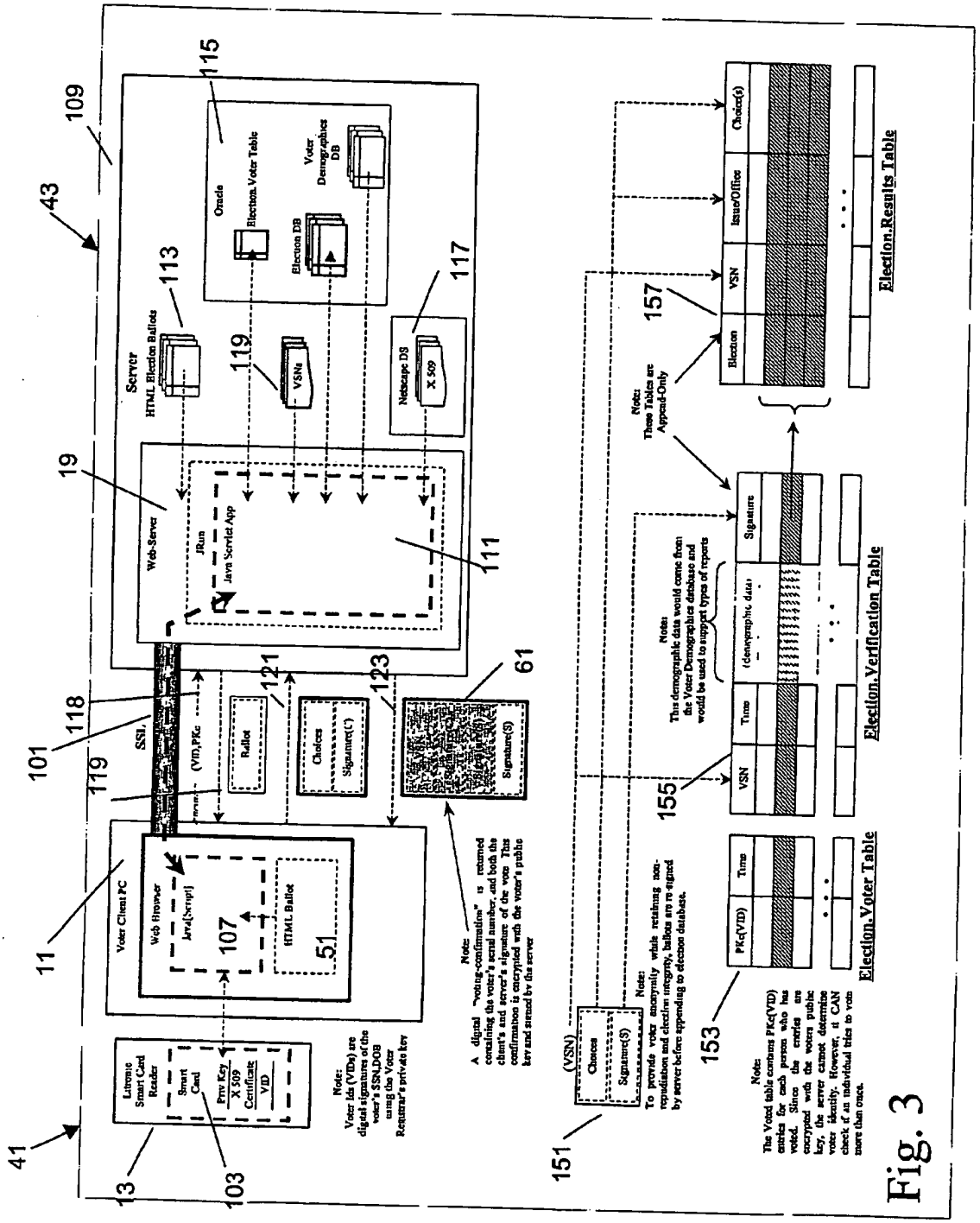

41
43
109
115
113
117
119
19
111
101
118
119
121
123
61
11
107
51
13
103
151
153
155
157
Server
HTML Election Ballots
Oracle
Election.Voter Table
Election DB
Voter Demographics DB
Netscape DS
X.509
VSNs
Web-Server
JRun
Java Servlet App
SSL
(VID,PKc
Ballot
Choices
Signature(C)
Signature(S)
Voter Client PC
Web Browser
Java[Script]
HTML Ballot
Electronic Smart Card Reader
Smart Card
Priv Key
X.509 Certificate
VID
(VSN)
Choices
Signature(S)
PKc(VID)
Time
VSN
(demographic data)
Signature
Election
VSN
Issue/Office
Choice(s)
Election.Verification Table
Election.Results Table
Note: Voter Ids (VIDs) are digital signatures of the voter's SSN,DOB using the Voter Registrar's private key
Note: A digital "voting-confirmation" is returned containing the voter's serial number, and both the client's and server's signature of the vote. This confirmation is encrypted with the voter's public key and signed by the server
Note: To provide voter anonymity while retaining non-repudiation and election integrity, ballots are re-signed by server before appending to election database.
Note: This demographic data would come from the Voter Demographics database and would be used to support types of reports
Note: These Tables are Append-Only
Note: The Voted table contains PKc(VID) entries for each person who has voted. Since the entries are encrypted with the voters public key, the server cannot determine voter identity. However, it CAN check if an individual tries to vote more than once.

Fig. 3

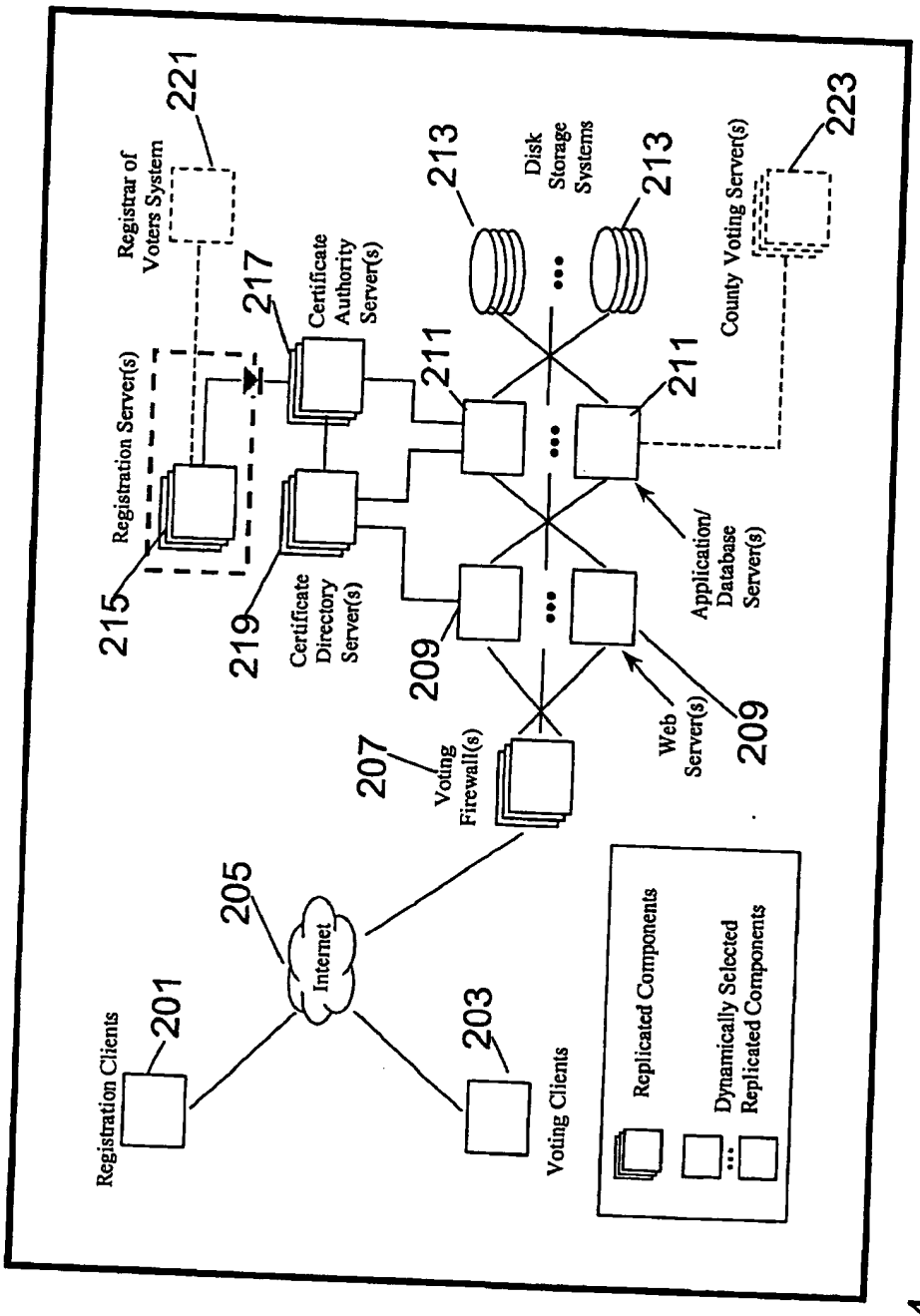

Registration Clients
201
Internet
205
Voting Clients
203
Voting Firewall(s)
207
Web Server(s)
209
Application/ Database Server(s)
211
Disk Storage Systems
213
Certificate Directory Server(s)
219
Registration Server(s)
215
Certificate Authority Server(s)
217
Registrar of Voters System
221
County Voting Server(s)
223
Replicated Components
Dynamically Selected Replicated Components

Fig. 4

METHOD AND SYSTEM FOR SECURING NETWORK-BASED ELECTRONIC VOTING

FIELD OF THE INVENTION

[0001] The invention relates to a method and system which provides the security techniques required to secure a voting system for use on a wide area network such as the global computer network, or on a local area network.

BACKGROUND OF THE INVENTION

[0002] The current approaches to provide a secure voting system on a wide area or local area network have traditionally emphasized purely cryptographic-protocol-based solutions to secure the voting. The work done to date is largely purely research into specific issues in secure electronic voting and does not address the practical application into a real-world system.

[0003] The prior art has approached worldwide area network, for example, on the global computer network known as the Internet™, elections as an extension of secure, electronic commerce techniques without providing a comprehensive approach to the significant threats, vulnerabilities and risks that threaten the security, authenticity and reliability of such elections.

[0004] Internet elections must achieve the objectives of conventional elections, specifically: "democracy" (only registered citizens may vote once in any election), accuracy (votes may not be altered, forged or deleted), "privacy" (no one may know how anyone else voted or prove how they voted), and "verifiability" (everyone should be able to verify their own ballot, as well as the correctness of the entire election). Moreover, Internet elections address additional capabilities: "mobility" (individuals should be able to vote from any Internet-accessible location, at any legal time), "convenience" (voting should be simple and convenient for everyone), and "flexibility" (the technology should be applicable to all elections).

[0005] Internet voting systems must achieve these objectives in the face of both conventional election threats, and threats specific to automated, distributed computer systems, including: fraud, abuse of privilege (privileged individuals may act inappropriately), denial of service (computer services may be impaired or rendered inaccessible), software flaws, tampering (of recorded ballots or other data), malicious software, wiretapping (sniffing, modification or replay of communications), vote selling, or masquerading (by client/server computers or by people).

[0006] The prior art has taken several approaches towards Internet election systems. Electronic commerce or E-Commerce approaches rely on securing communications through encrypted connections and verifying individual identity only through weak or single-factor authentication (e.g., passwords). Encrypted Absentee Balloting systems emulate conventional absentee balloting by using ballots that are doubly encrypted using symmetric keys. Cryptographic protocols, particularly those relying on asymmetric or public-key cryptography hold the greatest promise but have been relegated largely to the academic community.

[0007] All these techniques have characteristic weaknesses. E-Commerce techniques secure only voter-system communications. They provide weak authentication and no (strong) mechanisms for achieving democracy, privacy, accuracy or verifiability. Encrypted Absentee Ballot systems provide better privacy, but provide no stronger mechanisms for democracy, accuracy or verifiability, and are vulnerable to abuse of privilege, potentially compromising the keys used to ensure privacy. Many of the cryptographic protocols developed to date are complex, making implementation verification difficult. Public-key cryptography and digital signature techniques promise strong authentication, accuracy and verifiability. However, the generation and distribution of public-private (secret) key-pairs, and the protection of private keys, makes these techniques difficult to apply to large-scale applications such as Internet voting.

[0008] Specifically, it has been recognized that existing private-key management techniques, i.e., PKI approaches, are not acceptable if they require the end users to buy, install or configure anything, or require any particular type of client device. Such considerations become particularly significant when there may be huge numbers of end users, for example, 100,000 to 1,000,000, such as may be the case in an election.

[0009] It is recognized that PKI technology supports the use of public-key cryptography by providing various means to generate public-private (secret) key pairs, protect access to the private (secret) key so that it can be used only by the individual with whose identity it is associated, and provide for distribution and convenient access to the public key. Common strategy involves generation of public/secret key pairs on a user's personal computer by an application such as a web browser, storage of the private key within a personal identification number (PIN) protected, encrypted key-store file on the user's personal computer (PC), and exportation of the public key to a certificate authority, for example, where it is wrapped in a digital certificate, such as an X.509 digital certificate, and made available for public access on a lightweight directory access protocol (LDAP) certificate directory service.

[0010] This approach has advantages in that it is convenient and the private keys never leave the user's PC. Disadvantages result, however, because even though the private keys are protected in PIN-based encrypted files, PCs offer little protection against key-store cryptoanalysis by malicious software, and user mobility is impaired as it requires effort to export a private key so that it can be used on another platform.

[0011] An alternative strategy involves generation of public/secret key pairs on a secure platform rather than the user's PC, for example, a server. Yet still further, the approach involves storage of the private key, and perhaps other authentication-related data, on a storage device such as a password-encrypted floppy disk, or on a password-protected token/dongle, Java-ring (iButton) or smart card devices, as well as exportation of public keys and digital certificates as described with respect to the first approach.

[0012] One advantage of this approach is that the private key is more easily accessed from various computers, facilitating mobility, so long as there is a hardware interface for the private-key device. In addition, the private key is better protected within a removable device. Resultant disadvantages include the fact that the server must be verified not to make/leave copies of the private key. In addition, there must be some sort of hardware interface to allow retrieval of the key from the storage device, e.g., disk drive, USB port,

iButton/smart card reader, etc. Yet still further, these hardware interfaces may be expensive, difficult to install/configure, and may not be universally available, thus inhibiting mobility.

[0013] The advantages and disadvantages of the above-identified two approaches have led to a third approach. In the third approach, generation of public/secret key pairs is done on a secure platform other than the user's PC, for example, a server. The secret keys are stored in encrypted form on the secure server and downloaded to the client over a secure network connection as needed to support authentication, digital signature or encryption operations. The server must authenticate the user by some non-PKI-based method before allowing the user to download their private key. In most cases, this will still require some authentication device.

[0014] While providing further refinements and including advantages such as convenience and mobility being improved because private keys are always available from a network server, and no hardware interfaces are required on the client device, significant disadvantages still remain.

[0015] Initially, it is noted that there is a need for a secondary strong authentication technique that requires hardware token support, e.g., SecureID. In addition, such hardware tokens incur additional expense, and private keys are stored on a secure server using one or more keys known to the server, thus requiring the server to protect access to and use of these keys.

[0016] In all three approaches described, retrieval of private keys from local/network storage is required for use within the memory of a PC or thin-client device, and exposes the key to potential compromise. Only tokens with processors can perform the necessary cryptographic operations without exposing the private key. None of the approaches offer sufficient security, mobility and convenience at a sufficiently low cost to make public/private key cryptographic services, e.g., authentication, non-repudiation, encryption, attractive for applications with a potentially large number of users such as in the case of an election with users numbering from anywhere between 100,000 to about 10,000,000.

[0017] In order to make public/private key cryptographic services feasible for such applications, there must be a low-cost way to generate public/secret keys, while providing secure storage for and access to those keys without requiring special hardware or inconvenient procedures. These advantages and other advantages are provided by the system and method described herein, and numerous disadvantages of existing techniques are avoided.

SUMMARY OF THE INVENTION

[0018] In accordance with one aspect of the invention, there is provided a method of securely voting over a network, which can be a local area network, or a wide area network such as the global computer network known as the Internet™. The method involves delivering an electronic ballot from a server with a vote serial number on the ballot, to an individual at a terminal over a connection secured using both the server's and the voter's private keys. Thereafter, the ballot is filled in with the voter's choices, which are digitally signed using the voter's private key. The voter's ballot choices, bearing the voter's electronic signature, and the vote serial number is then delivered to the server. A data element is then created from the individual's digital signature of the ballot choices, the server's digital signature of the voter's ballot choices (created using the server's private key) and the vote serial number to allow recording of the subset of the ballot in a data store at the server, and retaining the ballot information as a vote. This data element is then digitally signed using the server's private key to ensure its integrity and authenticity.

[0019] As described herein, the terms "individual", "user", "client", and "voter" are used interchangeably, and refer to a person on their own terminal which can be a personal computer or other like device on which voting in accordance with the method and system herein is achieved.

[0020] In a more specific aspect, the retention of the vote at the server can be confirmed by signing the individual's signature of the ballot, the server's signature of the ballot, and the vote serial number, and the signed confirmation is transmitted to the individual who submitted the ballot.

[0021] Yet still further, the method involves recording in the server's data store the server's digital signature of the ballot to allow verification at the server that all of the ballots cast have not been tampered with.

[0022] In a more specific application, while the ballots are initially described as being generated as an HTML document, to provide additional security, in an alternative form the ballot can be generated in bit-map form such that the intentions of the voter or individual voting may be determined by monitoring the (x,y) coordinates of their mouse-clicks on the ballot bit-map. This provides enhanced security, since to read bit-map documents requires advanced optical character recognition technology, which in turn requires and imposes a large computing power overhead, thus making malicious hacking into the system significantly more difficult and detectable.

[0023] In an alternative aspect, there is described a system for conducting secure voting over a network, for example, the global computer network known as the Internet, or on a local area network. The system includes a server having a data store associated therewith. The server is configured for connection to the network for communicating with terminals connected to the network. The server is further configured for delivering an electronic ballot having the vote serial number on the ballot, to an individual at a terminal connected to the network, and the ballot being configured for being filled in by the individual, and for having a subset thereof delivered to the server with the individual's electronic signature, and the vote serial number thereon.

[0024] Yet still further, the server is further configured for receiving the ballot choices and creating a data element from the electronic signature of the individual's ballot choices, the server's electronic signature of the individual's ballot choices, and the vote serial number to allow recording of the ballot choices in the data store and retained therein as a vote. This data element is then digitally signed using the server's private key to ensure its integrity and authenticity.

[0025] In a further aspect, the server is programmed for confirming retention of the vote at the data store by signing the individual's signature of the ballot choices, the server's signature of the ballot choices and the vote serial number,

and thereafter transmitting the signed confirmation to the individual who submitted the ballot.

[0026] Yet still further, the system provides that the server is programmed for recording in the data store the server's digital signature of the ballot choices for allowing verification at the server that all of the ballots cast have not been tampered with.

[0027] In a still further aspect, the system is capable of generating the ballot as either a bit-map or an HTML document. The advantage of the bit-map document is that tampering or hacking becomes more difficult because bit-map documents require optical character recognition as previously discussed, such that malicious hacking is not easily achieved without detection.

BRIEF DESCRIPTION OF THE DRAWINGS

[0028] Having thus briefly described the invention, the same will become better understood from the following detailed discussion presented herein, with reference to the appended drawings, in which:

[0029] **FIG. 1** is a system-level architectural view of how an operational system implementing electronic voting over a network, such as the global computer network known as the Internet, can be configured;

[0030] **FIG. 2** is a block diagram illustrating the flow of the electronic ballot and associated data elements between an individual or client side, and a server side, managing the electronic voting method;

[0031] **FIG. 3** is a block diagram showing in greater detail the components, and data information exchange illustrated in **FIGS. 1 and 2**; and

[0032] **FIG. 4** is an architectural diagram showing in greater detail how a system and method as described herein could be deployed on a broad basis on a network such as the global computer network known as the Internet.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

[0033] **FIG. 1** is a system-level architectural view of how an operational system and method as described herein might be implemented. The client personal computer **11** or PC **11**, typically a personal computer running an operating system such as Microsoft Windows™, which may optionally include a smart card reader **13** connected thereto, although this is not required. The PC **11** includes network access capability which can be to the local area network, or to a global computer network **17**. In the case of a global computer network **17**, the PC **11** would have access to the global computer network **17** through, for example, an Internet service provider (ISP) **15**, or alternatively, access to other parts of the network might be through a direct cable modem, or a local, or a network attachment to the global computer network **17**.

[0034] On the server side, there is provided a primary interface to the entire system through a web server **19** in a conventional manner which is well known to those of ordinary skill in the art, and which is common to most electronic commerce architectures. The web server **19** interoperates with a certificate authority **21**, which can be for example, an enterprise server suite such as that available from Netscape Corporation. The certificate authority **21** uses a certificate-generating system, such as one like that available commercially under the name iPlanet, which is conventional, and which is one of many alternatives which can be used to implement the functionality described herein.

[0035] In addition, the web server **19** can also interoperate and be connected to a back end application or database server **23** and an LDAP certificate directory server **25**.

[0036] With respect to the LDAP certificate directory server **25**, by way of explanation, it can provide a certificate such as an X.509 certificate, which is a text file that is used to contain information about an individual, together with an encoding of the individual's public encryption key to the system described herein. The certificate file is then digitally signed by the certificate authority **21** that issued it. If it is desired to use the public keys of a number of individuals in an open context, there has to be a way of accessing the X.509 certificates. This can be done by placing them on a light-weight directory access protocol server (LDAP) such as the LDAP certificate directory server **25** shown, through which access to those certificates can be provided. For example, LDAP servers are provided commercially through a number of entities, and it is possible to obtain from such servers another party's public key certificate, for example, if it is desired to provide digitally signed, encrypted electronic mail.

[0037] More specifically, LDAP is a protocol on a data architecture for storing name-value pairs and on an LDAP certificate directory server **25** there would be stored certificates, such as X.509 certificates bound to each individuals' name.

[0038] With respect to the application database server **23**, it is also conventional and well known to those of ordinary skill in the art. Such an application database server **23** can be implemented using Java Servlets or Enterprise Java Beans (EJBs), which are typically small packets of functionality to make it easy and more efficient to use the more sophisticated Java implementation of web server **19** functionality. In operation, the web server **19** receives a request for a certain web page and in that web page is a reference to some call onto a piece of Java functionality that is written as a Java Servlet. An architecture known generally as the application database server **23** architecture allows the web server **19** to call functionality in the database server using Java Servlets or EJBs **23**. The application/database server **23** is typically a separate machine that is specifically optimized to support the invocation of that kind of functionality, encoded, for example, as Java Servlets. . More particularly, the application database server **23** allows invoking of pre-compiled and packaged functionality that is written in the form of Java Servlets, EJBs, or some other type of reusable component.

[0039] In the case of the present system and method, the reusable functionality will involve, for example, delivery of a ballot, which can be either in the form of an HTML or XML document, or for enhanced security as will be described hereafter, in the form of a bit-map.

[0040] Thus, when a user interacts with the web server **19** from their PC **11**, a Servlet, or one or more EJBs, processes the request for the user to register with the system, including a request to cast a ballot. The Servlet or EJBs that are

invoked present the ballot to the user, and handle the interaction with the user in the course of casting the vote.

[0041] If it is desired to look at the results of an election, another Servlet or a different set of EJBs can be invoked to support that functionality. As may be appreciated by those of ordinary skill in the art, fine-grained packaging of functionality can be defined depending on the capabilities to be implemented as described hereafter.

[0042] In one implementation, a Registrar of Voters **27** may also be tied into the system and would be responsible for the registration of individuals who are legitimately, legally allowed to vote in a particular county. One way of conducting the registration is the conventional interacting in person with the Registrar of Voters, or through conventional mail. It is contemplated herein that such registration could be accomplished over the network, such as the global computer network **17**, in a manner that it may be desired to have an electronic interface to the Registrar of Voters **27**.

[0043] For example, one method of establishing the interface may be with a local Division of Motor Vehicles, particularly because of recent trends toward making the Division of Motor Vehicles responsible for identification and authentication of individual entities, and the Registrar of Voters appears to be an organization that might be able to use such capability.

[0044] As will also be appreciated, in the case of implementing an interface with the Registrar of Voters **27**, some kind of X.509 certificate exchange as discussed previously could also be implemented, and the use of certificates would serve to authenticate any sort of interaction with the Registrar of Voters **27**. In addition, if an individual submitted a registration or request, it could be digitally signed and thus would require the individual's public key certificate in order to validate the signature.

[0045] In all cases, it would be required to digitally sign some electronic document, and the digital signature would have associated with it a well-known identity which can be looked up on a server such as an LDAP certificate directory server **25** to obtain the public key certificate corresponding to the claimed identity, and to then verify that the digital signature is actually a signature that could only have been generated by the individual having the claimed identity.

[0046] This is all standard public key infrastructure technology and well known to those of ordinary skill in the art. In the case of the Registrar of Voters **27**, this could be done through a certified agent for registering the voters, and there might be several methods by which such agents could be implemented and authorized by the Registrar of Voters **27**. Irrespective of what system is implemented, the agent would be acting as a front end to the Registrar of Voters **27**, and proxying the registration to them, and so, it would have to be legally authorized to do so.

[0047] While on the server side a number of different individual functional components are shown, it will be appreciated as an alternative that all the functions can be implemented on a single server, or depending on the size of the system, the functions can be allocated to separate servers which themselves may be replicated. This is an alternative architectural approach well known to those of ordinary skill in the art, and only for the sake of clarity has the system been shown in **FIG. 1** as separate boxes, which could be co-located on a single machine or duplicated or replicated on multiple boxes depending on the load and degree of redundancy and tolerance desired.

[0048] **FIG. 2** illustrates in block diagram form the data and information flow which will occur in a system and method as described herein. The components of data flow are shown divided by a dashed line **45** which separates the client **41** side which relates to the individual and the individual's PC, and is separated from the server **43** side.

[0049] A ballot **51** is shown on the client **41** side which has been delivered from the server **43** side and can be some form of electronic document. The document can take various forms but for purposes of the description herein, the ballot **51** is assumed to be an HTML form document, although more secure type and untamperable documents such as bit-map representations can also be deployed in accordance with the system and method.

[0050] The difficulty in building a system and method for such voting is being able to verify that only a single individual can cast a ballot, that they can cast only one ballot, and that it cannot be tampered with or undetectably altered or detected in any manner. **FIG. 2** illustrates the essential implementation for being able to achieve these goals.

[0051] The ballot **51** is delivered, for example, to the home PC **11** through the web server **19** from the application database server **23**, all of which were previously described with respect to **FIG. 1**. Using the home PC **11**, through a web browser, an individual can go through and make selections on the ballot, and after pressing enter or casting the ballot, the individual's PC **11** transmits back a subset of that form consisting of the ballot choices and the voter's digital signature of the ballot choices, DS(B,c).

[0052] Thus as is shown in **FIG. 2**, in the top arrow line from the ballot **51**, the selection is delivered as a representation to the server side **55**. The ballot and response values are structured in a way that it is easy to read the response values and determine which issues or offices were being voted on, and what the selections were. Those values are parsed and stored into a relational database, the structure of which will be described hereafter with reference to a separate figure. When the ballot is received on the server side **43** as shown by the dashed line box **53**, the server computes DS(B,s), a digital signature of the ballot using the server **43** private key.

[0053] In **FIG. 2**, in labels such as DS(. . . ,C) or DS(. . . ,c), an upper case letter means a public key, and a lower case letter means a secret or private key, so that in any particular block, this refers to the fact that when a ballot is received, the server creates a digital signature of the ballot using the server's secret or private key. On the client **41** side, when an individual casts a ballot **51**, the client **41** side creates a digital signature of the ballot **57** using the individual's secret or private key. Thus, both of these signatures, one created by the individual, and the other created by the server, can only have been created by the respective entities because they are both signatures that are created using the respective secret or private keys.

[0054] The individual's signature of the ballot is then delivered to the server **43** side where it is combined with three other elements at block **59**. Specifically, the server's

signature **53** is combined with the individual's signature **57** along with a vote serial number (VSN) which is, for example, like a ballot serial number and can be an arbitrary number that goes from one to infinity. The vote serial number can be generated per election, and has no relationship to the voter, and is just an incidental sequence number that indicates a vote delivered in the election. Those three elements are then digitally signed by the server yielding DS(C,s), and the four combine into an aggregation of core components which is a ballot confirmation token. This allows confirmation that a particular ballot has been retained in the system and no tampering has occurred. That token is then transmitted back to the individual as a confirmation token **61**. The confirmation token **61** can then be encrypted with the individual's public key, thus rendering it undecipherable to anyone except the individual.

[0055] Such encryption is not mandatory but may be desirable, depending on other specific implementations of the system and method. For purposes of the disclosure herein, it is noted that while the term "token" is referred to, it could be characterized as a data element which is the signature confirmation by the server, in particular, the confirmation which has three components and a digital signature. Thus, by tying these components together, and having the server sign the components, if later on someone submits the confirmation, the server can verify that the confirmation was issued by the server, minimizing the possibility that confirmations can be forged.

[0056] On the server **43** side, the server's digital signature is also recorded along with the vote or ballot as shown at block **55**. If it becomes desirable to verify that all of the ballots cast in the election have been untampered with, that can be done on the server **43** side using only the contents of the database and the server ballot signatures which have been recorded in the data store.

[0057] This is further illustrated by arrow **63** which illustrates universal verifiability. More specifically, a search is conducted through the database in a manner indexed to a vote serial number, and for each vote serial number, a ballot is reconstructed. The reconstructed ballot has no identification back to the voter and is completely anonymous. However, the ballot responses are the same as those that the individuals generated when the ballot was cast. A digital signature can then be created over the reconstructed ballot using the server's public key, and that signature can be verified against the signature that was recorded when the individual cast the ballot that was created using the server's private key. Thus, the arrow **63** represents the validation of the server's ballot signature created with its private key, against the server's ballot signature that was generated from the reconstructed ballot using the server's public key. This can be done for all of the ballots stored in the system, and thus, it can be verified that none of the ballots have been tampered with at any point in time after a ballot has been cast. This is referred to as universal verifiability, which refers to the property that allows for verification that for all voters none of the ballots have been forged, deleted or altered.

[0058] Consider now the case where an individual would want to connect to the system, i.e., on the server **43** side to determine if their ballot vote is properly recorded. In such a case, the individual can present vote confirmation **61** through a transmission **67** to the server **43** side. Of course, the individual will have to decrypt the confirmation **61** as previously discussed using their private key. The confirmation is then presented to the system which decomposes the confirmation into four components, which are represented by blocks **69**, and have been previously discussed with reference to blocks **59** and **61**.

[0059] The digital signature on that confirmation can then be recomputed, and it can be verified that the confirmation has not been altered. Having done so, the vote serial number can then be extracted from the confirmation, and the database can be indexed to allow reconstruction of the voter's ballot exactly as cast.

[0060] The two horizontal arrows **71** and **73** illustrate what is known as individual verifiability. The server's ballot signature can be extracted out of the confirmation and validated against the server's ballot signature that is generated from the reconstructed ballot. This is demonstrated by the exchange which occurs through arrow **71**. The individual's ballot signature that was computed using the individual's private key can also be validated by the comparison represented by arrow **73** against the digital signature that has taken over the reconstructed ballot using the voter's public key. This can be done because the communication between the individual and the server is protected, as illustrated later in **FIG. 3**, by a secure socket layer (SSL) connection **101** that provides temporary access to the individual's public key.

[0061] In fact, in such an implementation, the public key of the individual on the individual's end of the connection can be obtained outside of the system and once it is known what the individual's public key is, the requirement for an LDAP certificate directory server **25** to obtain the public key can be eliminated.

[0062] As may be appreciated from the discussion of individual verifiability, in contrast to universal verifiability, individual verifiability provides two ways of verifying by using either the server's digital signature or the individual's digital signature on the ballot.

[0063] **FIG. 3** shows in greater detail the general architecture shown in **FIG. 1**, and the data flow shown in **FIG. 2**. Specifically, the upper part of **FIG. 3** shows the various components of the system along with boxes showing the data flow, with the lower portion of **FIG. 3** showing in greater detail the various resultant tables assembled with ballots that have been cast.

[0064] A smart card reader **13** can be implemented connected to an individual's PC **11** on a smart card **103** which is read by the smart card reader **13**, and can have stored thereon an individual's private (or secret) encryption key. A certificate such as an X.509 certificate for their public key, and their voter identification number which is an arbitrary sequence number generated when they register with the system, can also be stored on the smart card **103**. The individual's PC **11** will typically be running a standard web browser **105**, such as is commercially available from Netscape Corporation, and inside the web browser **105** is a Java script interpreter **107** with the ballot **51** presented within the web browser **105**. Although the ballot has been previously described, and is illustrated in **FIG. 3**, as an HTML or XML document, it can also take other forms such as a bit-map, if enhanced security is desired.

[0065] While a personal computer **11** has been shown with a standard commercially-available browser **105**, it may also be appreciated that such browsers are often not sufficiently secure. Thus, as contemplated herein, it is also possible to implement in a manner well known to those of ordinary skill in the art, a non-commercial browser which avoids the security pitfalls of currently-existing commercial browsers.

[0066] More specifically, it is common for malicious software to read/modify sensitive files on unsecure personal computers. Such unsecure personal computer platforms can include those which are Intel processor/Microsoft Windows operating system, or Apple MacIntosh operating system-based. Specifically, in such commercial systems, the security ends at the client. As a result, the entire system may be vulnerable to attack by malicious software executing within the individual's PC. With no individual platform security mechanisms, such attacks could detrimentally impact information confidentiality, integrity, authenticity, or availability within the overall system.

[0067] In order to address such a problem which may be inherent in a conventional commercial web browser, and with ballots such as an HTML or XML document ballot **51**, a protocol can be implemented that combines anonymous context, and visual obfuscation to make it virtually impossible for malicious software to knowledgably and undetectably interfere with a concurrently executing individual PC application in order to impact information confidentiality, integrity and authenticity.

[0068] In accordance with the specific implementation of such security as contemplated herein, and as will be readily apparent to those of ordinary skill in the art, cryptographic techniques, protocols and data representation can be implemented in order to increase the work required of malicious software beyond what can be accomplished within a voting session at an individual's personal computer **11**. Specifically, implementation of visual obfuscation is intended to defeat the ability of malicious software to determine or alter network content. Such a technique would include but not be limited to variation of text, font, size, spacing, etc. The wording of the text associated with ballot choices, the location of graphic components, the shape of image of choice/selection targets, explicit or implicit relationships between graphical elements, and in some cases, color, can also be implemented in an obfuscating manner. In addition, a technique for converting content in HTML or XML format to image format can be employed as will be readily apparent to those of ordinary skill in the art, making it difficult, with current OCR algorithms to intercept and alter the limited ballot information being transmitted. Such OCR techniques are generally processor intensive, and thus attempts by malicious software to alter or interpret such ballot information would be readily detected.

[0069] Thus, as shown in the **FIG. 3** a voter ID and the public key of the individual is transferred at **118** over an SSL connection **101** to the web server **19** on the server **43**. The server side **43** which includes a number of function boxes assembled as one box **109**. The web server **19** which includes an execution environment for Java Servlets **111** then sends a ballot **119** obtained from a collection of ballots **113**, to the individual PC **111** through a transmission **119**. The individual then marks the ballot and returns the ballot as shown with arrow **121** with the choices thereon. The confirmation shown as block **61** is then returned as shown by arrow **123**.

[0070] It will be appreciated that within the collection **109** of function boxes, separate functionality and information is provided, for example, from the collection of election ballots **113**, vote serial numbers **119**, and certificates **117**, characterized preferably as X.509 certificates. In the Figure, block **115** is typically the application database server **23** shown in **FIG. 1** and serves to compile the election voter table, election database and optionally, a voter demographics database, all of which will be described hereafter with reference to the lower half of **FIG. 3**.

[0071] More specifically, the lower half of **FIG. 3** illustrates how the various pieces of information/data are assembled. At block **151** it is seen that to provide voter anonymity, while retaining non-repudiation and election integrity, ballots are re-signed by the server before appending to the election database. In this case, at box **151**, there are reflected the choices the individual ballot items that the individual voter casts a vote for, and are stored in an election results table **157**.

[0072] Table **157** conceptually includes four columns. The first column is the election in which the votes are cast. A separate database can be created per election but could also be done in this manner. The table **157** is indexed by the vote serial number (VSN), the issue or office being voted on, and the choice the individual makes. Thus, this is the table in which the ballot choices are stored. The voter's serial number is also stored in a table **155** which is an election verification table. The purpose of this table is to retain the digital signatures that protect the integrity of the ballot and the election verification table has at least three columns and perhaps others. The election verification table is indexed by the vote serial number. It includes a column for time and a column for the digital signature. Optionally, demographic data could also be input into the election verification table **155** as long as this information would not, through inference or aggregation, divulge the voter's identity.

[0073] On the left side is shown the election voter table **153** which is a hashed table that in order to achieve single-vote verification, to ensure that individuals cannot vote multiple times, provides that the voter identification or ID is encrypted or hashed using a one-way transform. One option is to employ an encryption using the individual voter's public key, but any one-way transform would work. The contents of the table **153**, since they are generated by a one-way hashed function are not reversible, so it is impossible to look into the table to see who voted. However, if an individual tries to vote more than once, the hash entry will collide with any new attempt to cast a second vote, and thus, there is provided a way of detecting a subsequent voting attempt without divulging anything about the identity of the individual.

[0074] Turning now to **FIG. 4**, there is illustrated in block diagram form a large-scale production voting system architecture. Registration clients **201** at their personal computers are shown as able to register through connection through the global computer network **205**, through a voting firewall **207**, web servers **209** and application database servers **211**, which may be ultimately connected to a Registrar of Voters system **221**. The Registrar of Voters system **221** may provide

registration information to a registration server **215** which cooperates as previously described with certificate directory servers **219**, and certificate authority servers **217**, and in cooperation with the other elements to allow delivery of a ballot to voting clients **203** to accomplish voting as previously described herein.

[**0075**] Having thus generally described the invention, the same will become better understood from the following claims in which it is set forth in a non-limiting manner.

1. A method of securely voting over a network, comprising:

delivering an electronic ballot from a server with the vote serial number on the ballot, to an individual;

filling in the ballot and creating a set of ballot choices that are digitally signed using the individual's secret key;

delivering the ballot choices with the individual's electronic signature, and the vote serial number to the server; and

creating a data element from the individual's electronic signature over the ballot choices, the server's electronic signature over the ballot choices and the vote serial number to record the ballot choices in a data store at the server, and retaining the ballot choices as a vote.

2. The method of claim 1 further comprising confirming the retention of the vote at the server by signing the individual's signature of the ballot, the server's signature of the ballot and the vote serial number, and transmitting the signed confirmation to the individual who submitted the ballot.

3. The method of claim 1, further comprising: recording in the server's data store the server's digital signature of the ballot to allow verification at the server that all of the ballots cast have not been tampered with.

4. The method of claim 3, further comprising: verifying for all individuals voting that none of the ballots have been tampered with by reconstructing the ballot for each individual using the vote serial number, creating a digital signature over each reconstructed ballot by using the server's public key, and verifying the digital signature against the ballot signature using the server's private originally recorded when the individual created and submitted the ballot with the individual's private key and verifying the digital signature against the ballot signature originally recorded when the individual created and submitted the ballot, digitally signed with the individual's private key.

5. The method of claim 2, further comprising: allowing the individual to verify that their ballot is retained in the server's data store accurately reflecting the way it was cast by presenting the confirmation to the server; decomposing the confirmation into the individual's signature of the ballot, the server's signature of the ballot, the vote serial number and the server's signature which resulted in the confirmation; recomputing the server's signature on the confirmation to ensure the confirmation has not been altered; extracting the vote serial number out of the confirmation if it has been verified that the confirmation has not been altered; and indexing a database in the server to allow reconstruction of the individual's ballot as it was cast.

6. The method of claim 5, further comprising: storing the individual's private encryption key, a certificate for the individual's public key and a voter identification generated when the individual registers with the system on a portable storage device; and reading the information on the portable storage device before allowing a ballot to be cast.

7. The method of claim 6, wherein said portable storage device is a smart card, and further comprising reading the information on the smart card before allowing a ballot to be cast.

8. The method of claim 6 wherein said certificate is an X.509 certificate.

9. The method of claim 1, further comprising: entering demographic data onto the ballot and storing the demographic data in relation to the ballot stored by the server.

10. The method of claim 1, further comprising: creating an election voter table at the server from encrypted individual's voter identification; and comparing each ballot to the encrypted individual's voter identification to detect if an individual attempts to cast more than one ballot.

11. The method of claim 1 wherein said ballot is a bit-map.

12. The method of claim 1 wherein said ballot is an HTML or XML document.

13. A method of securely voting over a network, comprising:

delivering an electronic ballot from a server with the vote serial number on the ballot, to an individual;

filling in the ballot and creating a set of ballot choices that are digitally signed using the individual's secret key;

delivering the ballot choices with the individual's electronic signature, and the vote serial number to the server;

creating a data element from the individual's electronic signature over the ballot choices, the server's electronic signature over the ballot choices and the vote serial number to record the ballot choices in a data store at the server, and retaining the ballot choices as a vote;

confirming the retention of the vote at the server by signing the individual's signature of the ballot, the server's signature of the ballot and the vote serial number;

transmitting the signed confirmation to the individual who submitted the ballot; and

allowing the individual to verify that their ballot is retained in the server's data store accurately reflecting the way it was cast.

14. A method of securely voting over a network, comprising:

delivering an electronic ballot from a server with the vote serial number on the ballot, to an individual;

filling in the ballot and creating a set of ballot choices that are digitally signed using the individual's secret key;

delivering the ballot choices with the individual's electronic signature, and the vote serial number to the server;

creating a data element from the individual's electronic signature over the ballot choices, the server's electronic signature over the ballot choices and the vote serial number to record the ballot choices in a data store at the server, and retaining the ballot choices as a vote;

recording in the server's data store the server's digital signature of the ballot to allow verification at the server that all of the ballots cast have not been tampered with; and

verifying for all individuals voting that none of the ballots have been tampered with.

15. A system for conducting secure voting over a network, comprising:

a server having a data store associated therewith, said server being configured for connection to the network for communicating with terminals connected to the network;

said server being further configured for delivering an electronic ballot having the vote serial number on the ballot, to an individual at a terminal connected to the network, and said ballot configured for being filled in by an individual, and for having a subset thereof corresponding to the ballot choices delivered to the server with the individual's electronic signature and the vote serial number thereon; and

the server being further configured for receiving the subset of the ballot and creating a data element from the individual's electronic signature over the ballot choices, the server's electronic signature over the ballot choices and the vote serial number to allow recording of the subset of the ballot within the data store and retained therein as a vote.

16. The system of claim 15, wherein: the server is further programmed for confirming retention of the vote at the data store thereof by signing the individual's signature of the ballot, the server's signature of the ballot and the vote serial number, and transmitting the signed confirmation to the individual who submitted the ballot.

17. The system of claim 15, wherein: the server is programmed for recording in the data store the server's digital signature of the ballot for allowing verification at the server that all of the ballots cast have not been tampered with.

18. The system of claim 17, wherein: the server is programmed for verifying for all individuals voting, that none of the ballots have been tampered with, by reconstructing the ballot for each individual using the vote serial number, creating a digital signature over each reconstructed ballot by using the server's public key, and verifying the server's signature over the ballot choices originally recorded when the individual created and submitted the ballot choices.

19. The system of claim 16, wherein: the server is configured for allowing an individual to verify their ballot is retained in the server's data store in a manner accurately reflecting the way it was cast in response to the individual presenting the confirmation to the server; for decomposing the confirmation with the individual's signature of the ballot, the vote serial number and the server's signature which resulted in the confirmation; recomputing the server's signature on the confirmation to ensure the confirmation has not been altered, extracting the vote serial number out of the confirmation if it has been verified that the confirmation has not been altered; and for indexing a database in the server to allow reconstruction of the individual's ballot as it was cast.

20. The system of claim 19, further comprising: a portable storage device configured for connection and transmission of information to the server, said information being an individual's private encryption key, a certificate for the individual's public key and a voter identification number generated when the individual registered to vote through the server; and the server being configured for receiving the voter ID and public key certificate from the portable storage device before allowing a ballot to be cast by the individual.

21. The system of claim 20, wherein: said portable storage device is a smart card, and further comprising a smart card reader connected to the individual's terminal.

22. The system of claim 20, wherein: the server is configured for processing an X.509 certificate, and wherein said certificate on the portable storage device is an X.509 certificate.

23. The system of claim 15, wherein: the server is programmed for generating a ballot which allows input of demographic data and for storing the demographic data in relation to each ballot stored.

24. The system of claim 15, wherein: the server is programmed for creating an election voter table from a one-way hash of individual's voter identification; and for comparing each ballot to the individual's hashed voter identification to detect if an individual attempts to cat more than one ballot.

25. The system of claim 15, wherein said server is programmed to generate said ballot as a bit-map.

26. The system of claim 15 wherein said server is programmed to generate said ballot as an HTML or XML document.

27. A system for conducting secure voting over a network, comprising:

a server having a data store associated therewith, said server being configured for connection to the network for communicating with terminals connected to the network;

said server being further configured for delivering an electronic ballot having the vote serial number on the ballot, to an individual at a terminal connected to the network, and said ballot configured for being filled in by an individual, and for having a subset thereof corresponding to the ballot choices delivered to the server with the individual's electronic signature and the vote serial number thereon;

the server being further configured for receiving the subset of the ballot and creating a data element from the individual's electronic signature over the ballot choices, the server's electronic signature over the ballot choices and the vote serial number to allow recording of the subset of the ballot within the data store and retained therein as a vote; and

the server being further programmed for confirming retention of the vote at the data store thereof by signing the individual's signature of the ballot, the server's signature of the ballot and the vote serial number, for transmitting the signed confirmation to the individual who submitted the ballot, and for allowing an individual to verify their ballot is retained in the server's data store in a manner accurately reflecting the way it was cast in response to the individual presenting the confirmation to the server.

28. A system for conducting secure voting over a network, comprising:

a server having a data store associated therewith, said server being configured for connection to the network for communicating with terminals connected to the network;

said server being further configured for delivering an electronic ballot having the vote serial number on the ballot, to an individual at a terminal connected to the network, and said ballot configured for being filled in by an individual, and for having a subset thereof corresponding to the ballot choices delivered to the server with the individual's electronic signature and the vote serial number thereon;

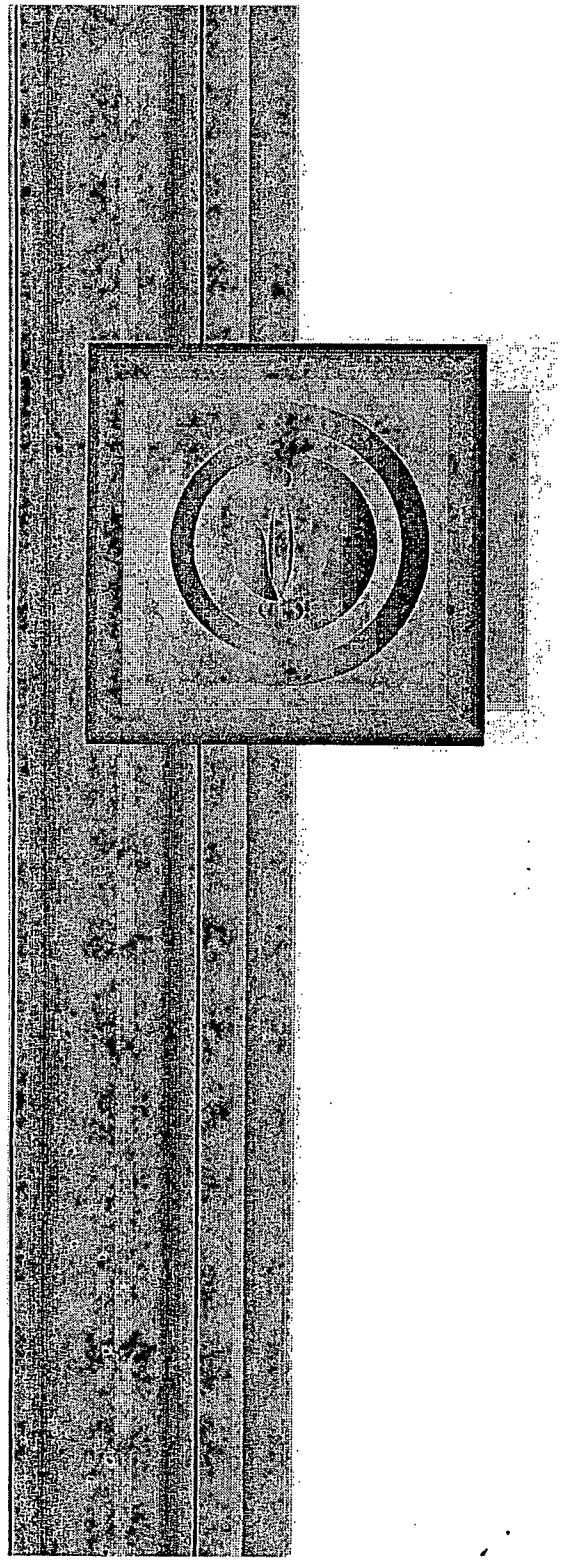
the server being further configured for receiving the subset of the ballot and creating a data element from the individual's electronic signature over the ballot choices, the server's electronic signature over the ballot choices and the vote serial number to allow recording of the subset of the ballot within the data store and retained therein as a vote; and

the server being programmed for recording in the data store the server's digital signature of the ballot for verifying at the server that all of the ballots cast have not been tampered with, by reconstructing the ballot for each individual.

* * * * *

EXHIBIT B

37 page document prepared prior to November 2002, entitled "Security in the System"

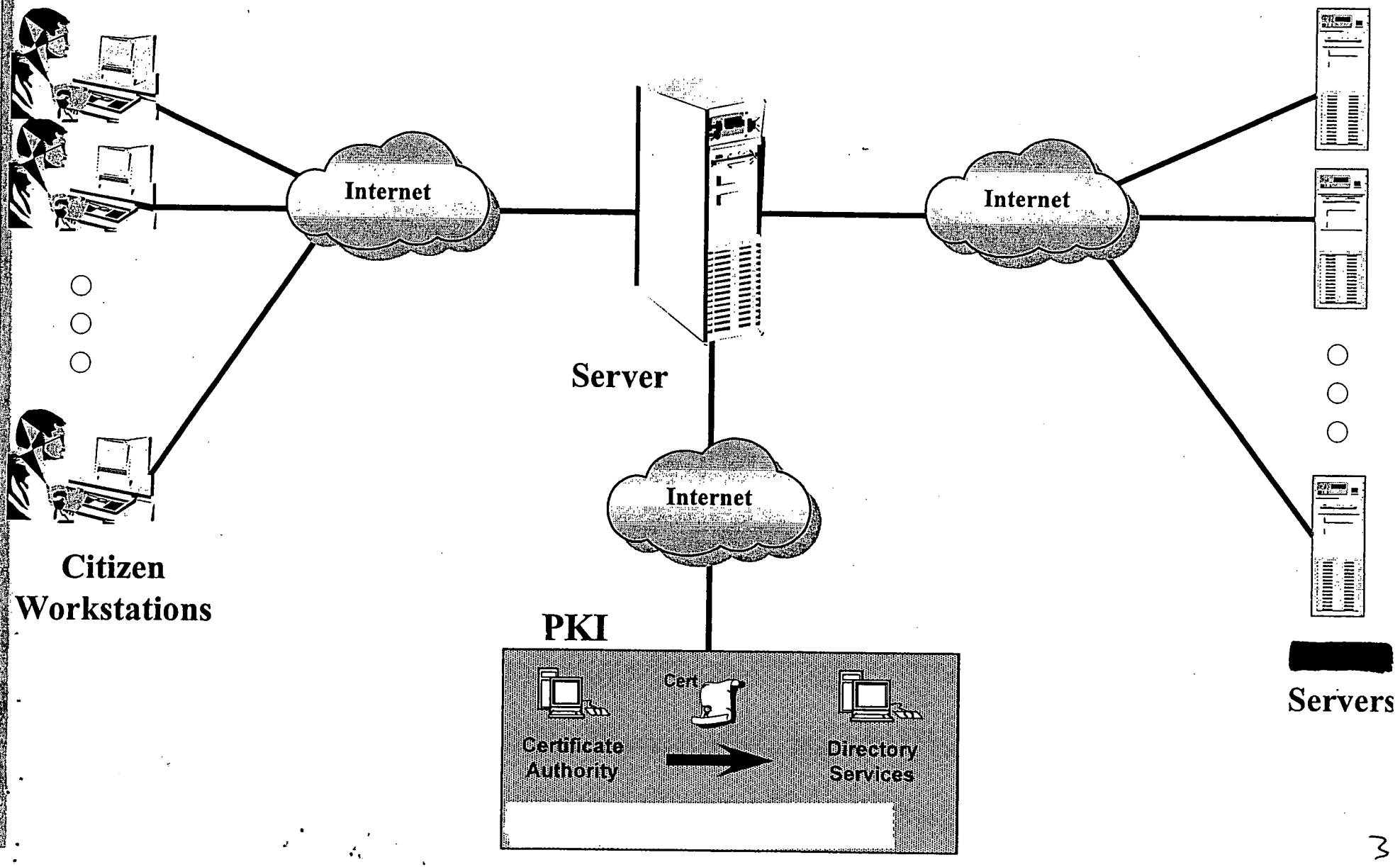


Security in the System

Requirements Review

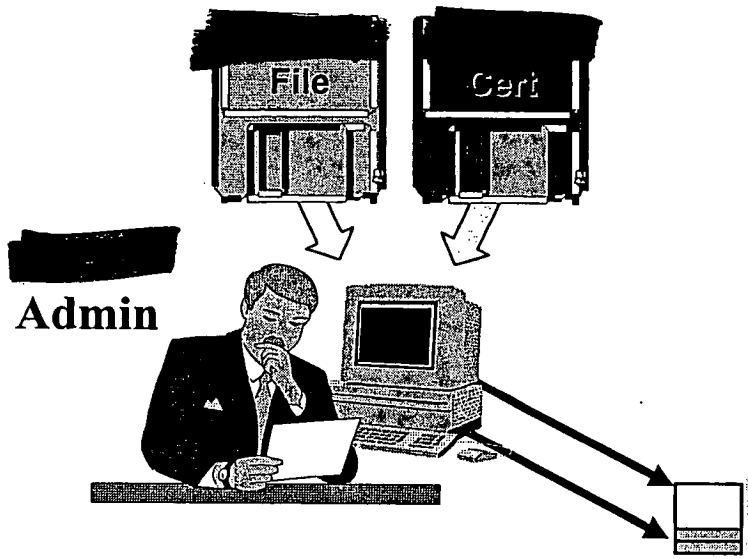
Reston, Virginia

Architecture



Object Security

Blank



Blank [redacted] Form

[redacted] Fields

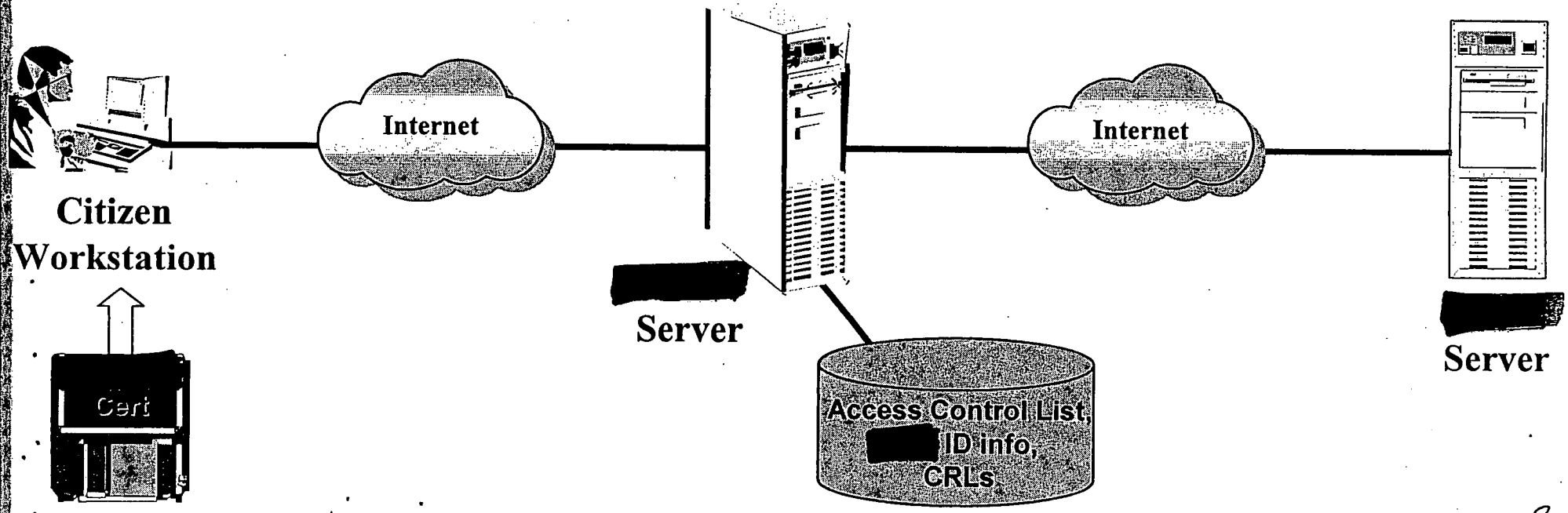
Mandatory Fields Marked

Specific Instructions

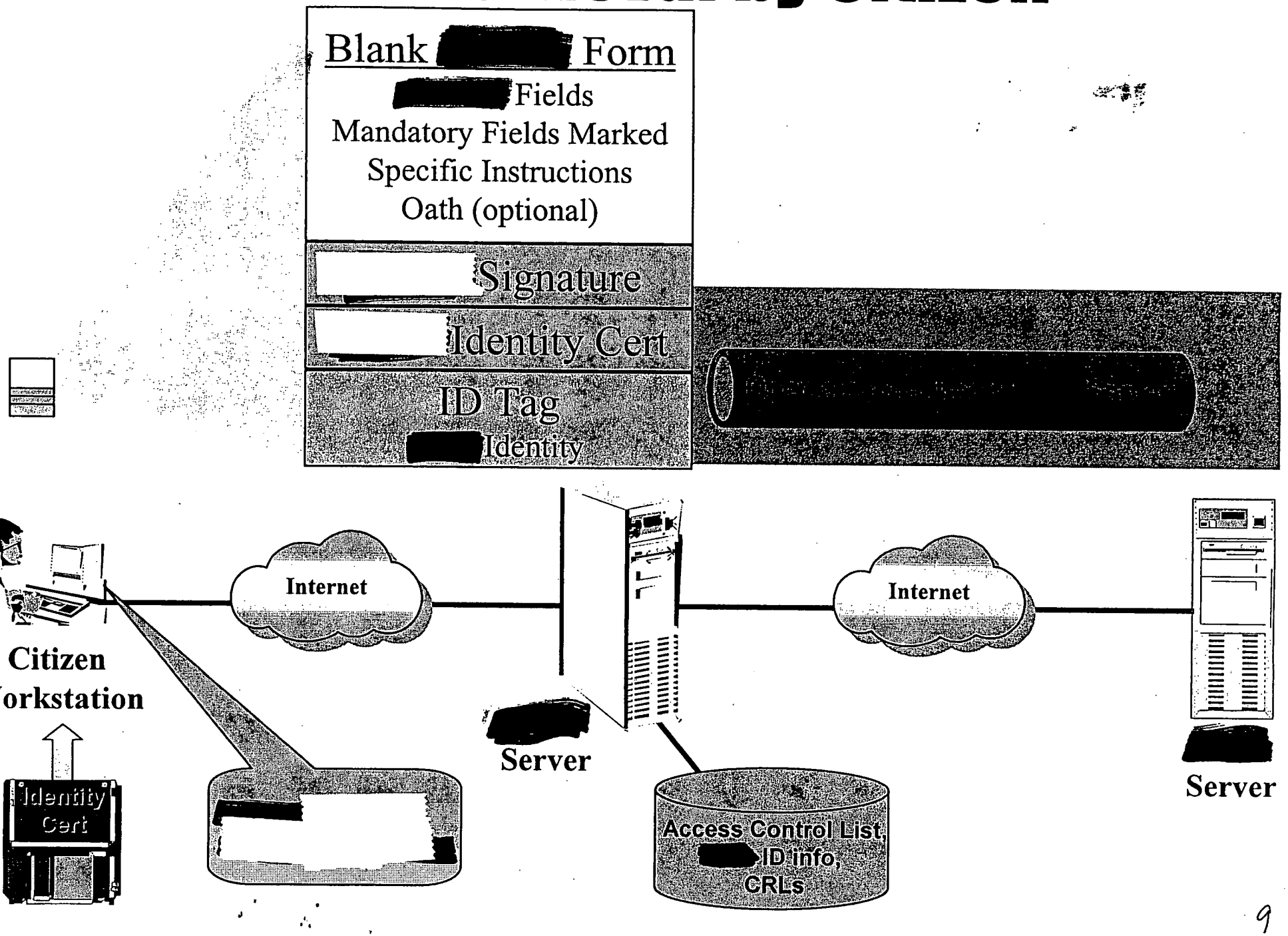
Oath (optional)

[redacted] Signature

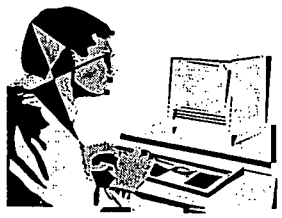
[redacted] Identity Cert



Blank [redacted] Retrieval by Citizen



Completing the Form



Citizen Workstation

Blank [redacted] Form

[redacted] Fields

Mandatory Fields Marked

Specific Instructions

Oath (optional)

[redacted] Signature

[redacted] Identity Cert

ID Tag [redacted] Identity

+ Personal Information =

Verify

Completed [redacted] Form

Completed Fields

Mand. Fields Verified

Oath Attested

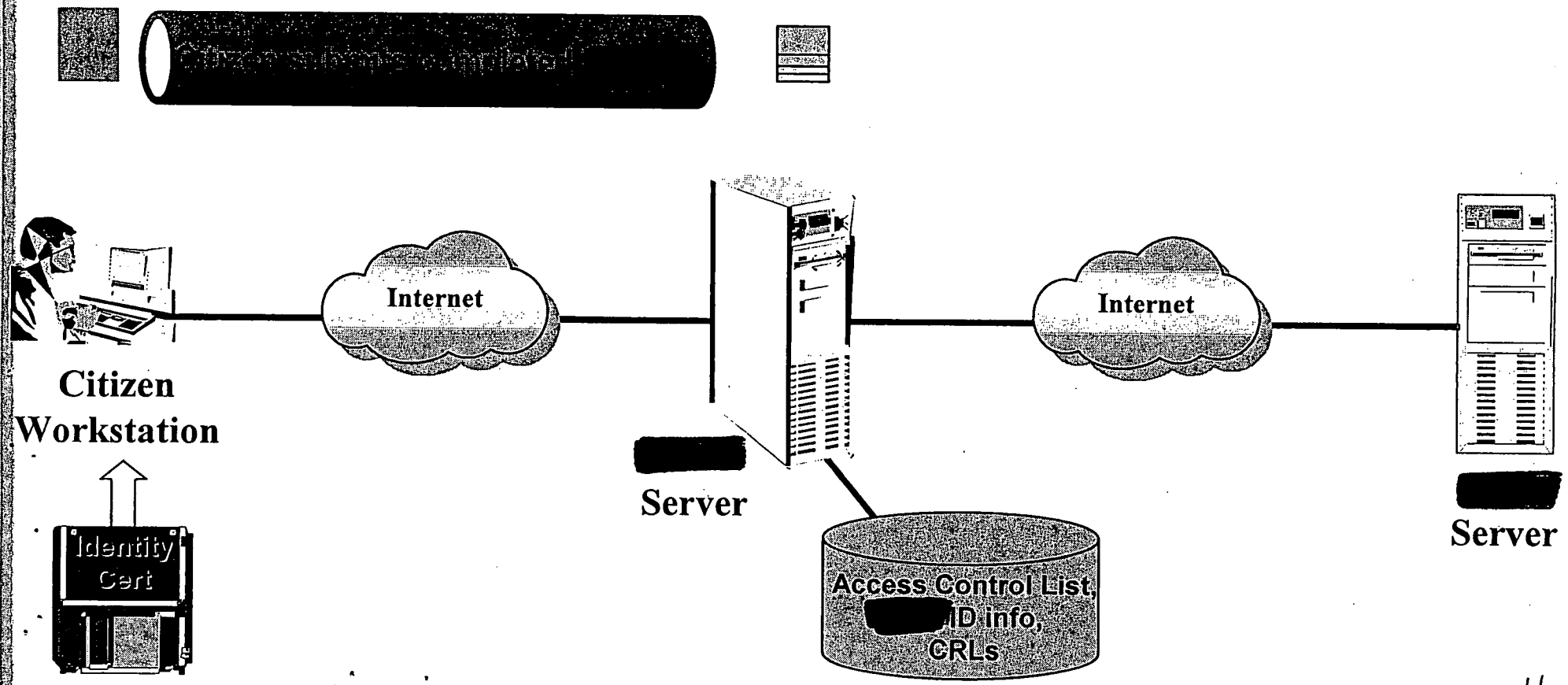
ID Tag [redacted] dentity

Citizen Signature

Citizen Identity Cert



Completed [redacted] Submission



Validating the Citizen

Completed [redacted] Form
Completed Fields
Mand. Fields Verified
Oath Attested

ID Tag
[redacted] Identity

Citizen Signature

Citizen Identity Cert

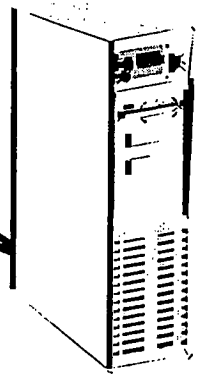
Postmark

[redacted] Signature

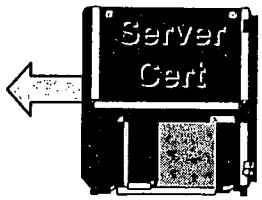
[redacted] Server Cert

Verify

Add



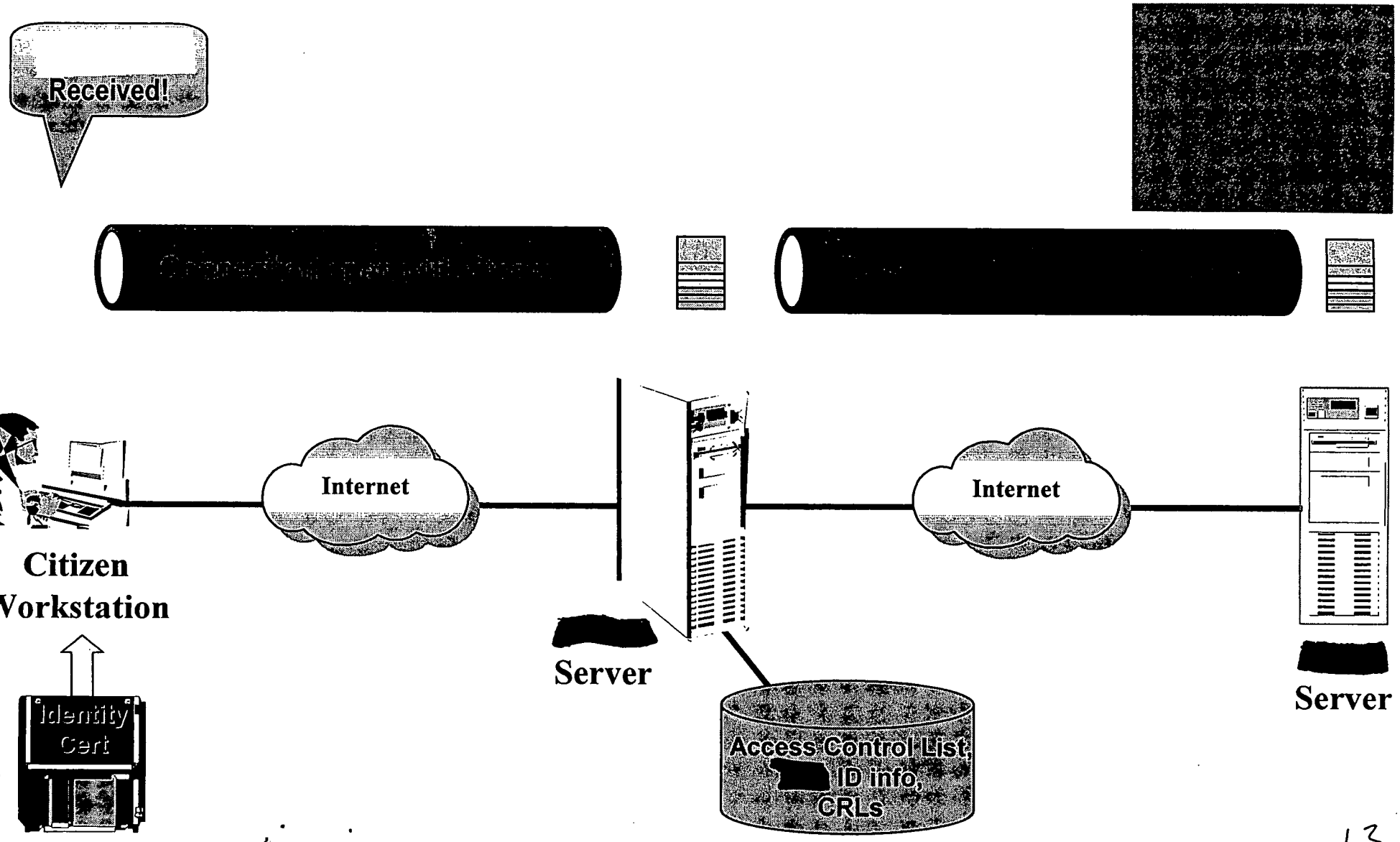
Server



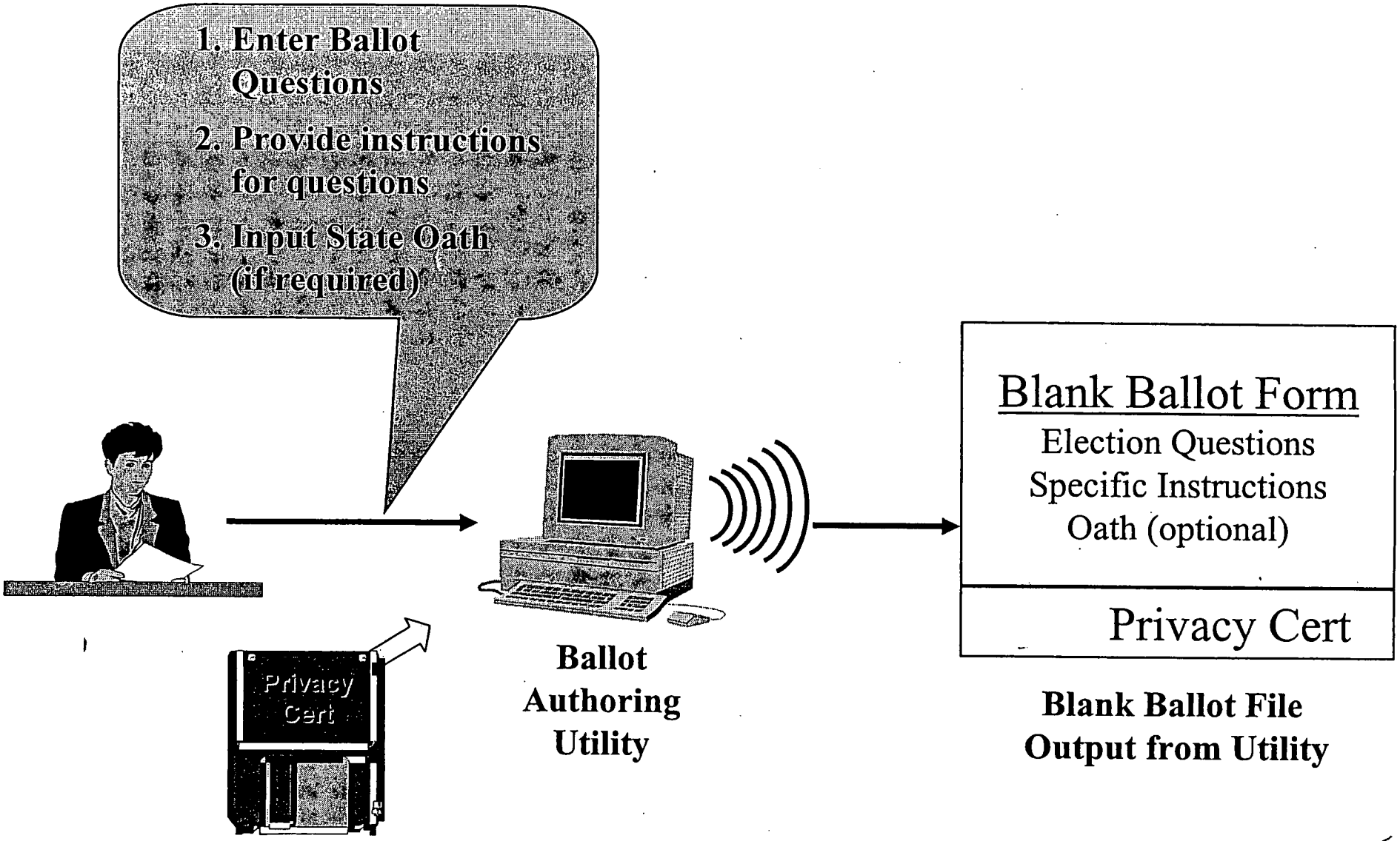
To Validate Certificate

- Check Validity Period ☑
- Verify Cert Chain ☑
- Verify Not On CRL ☑

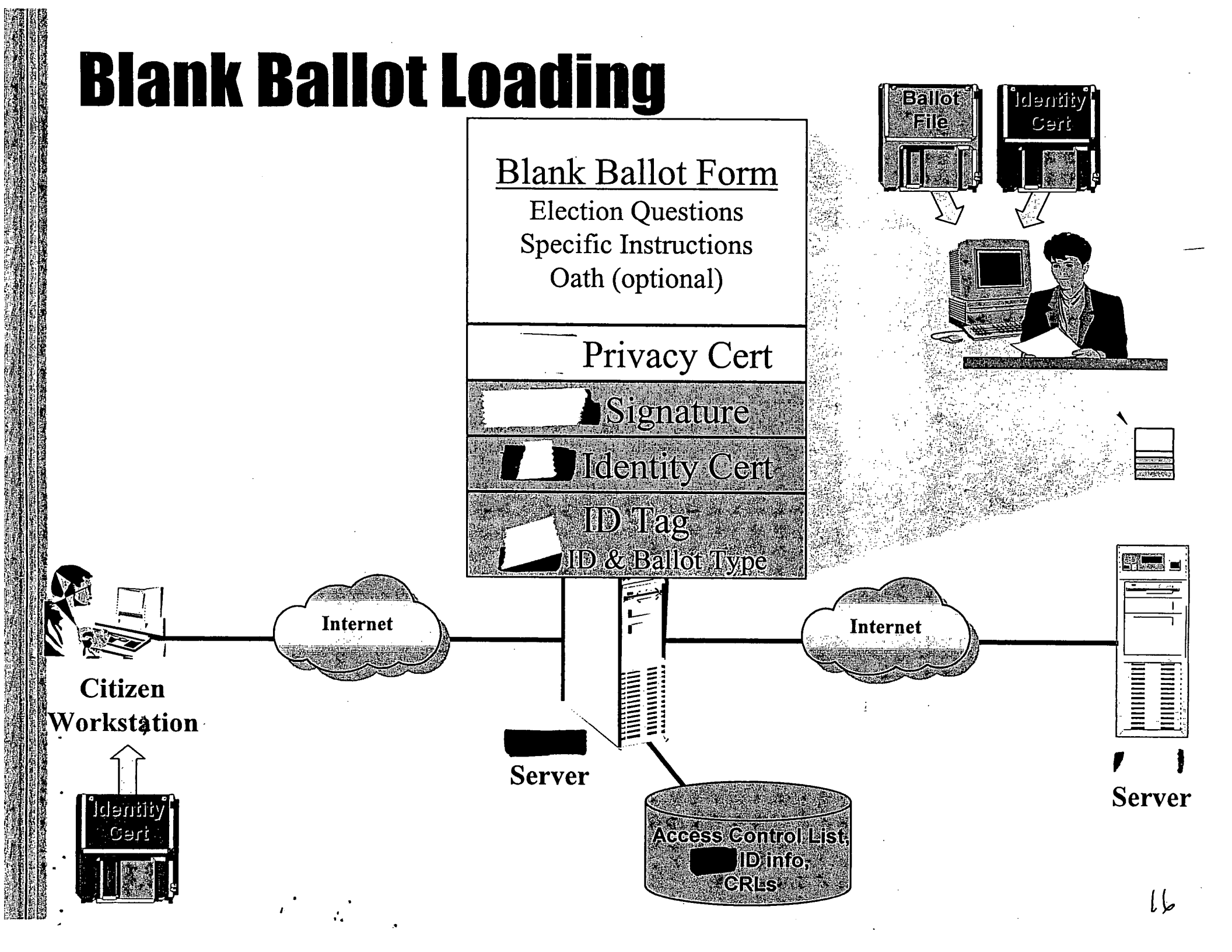
Completed Forwarding



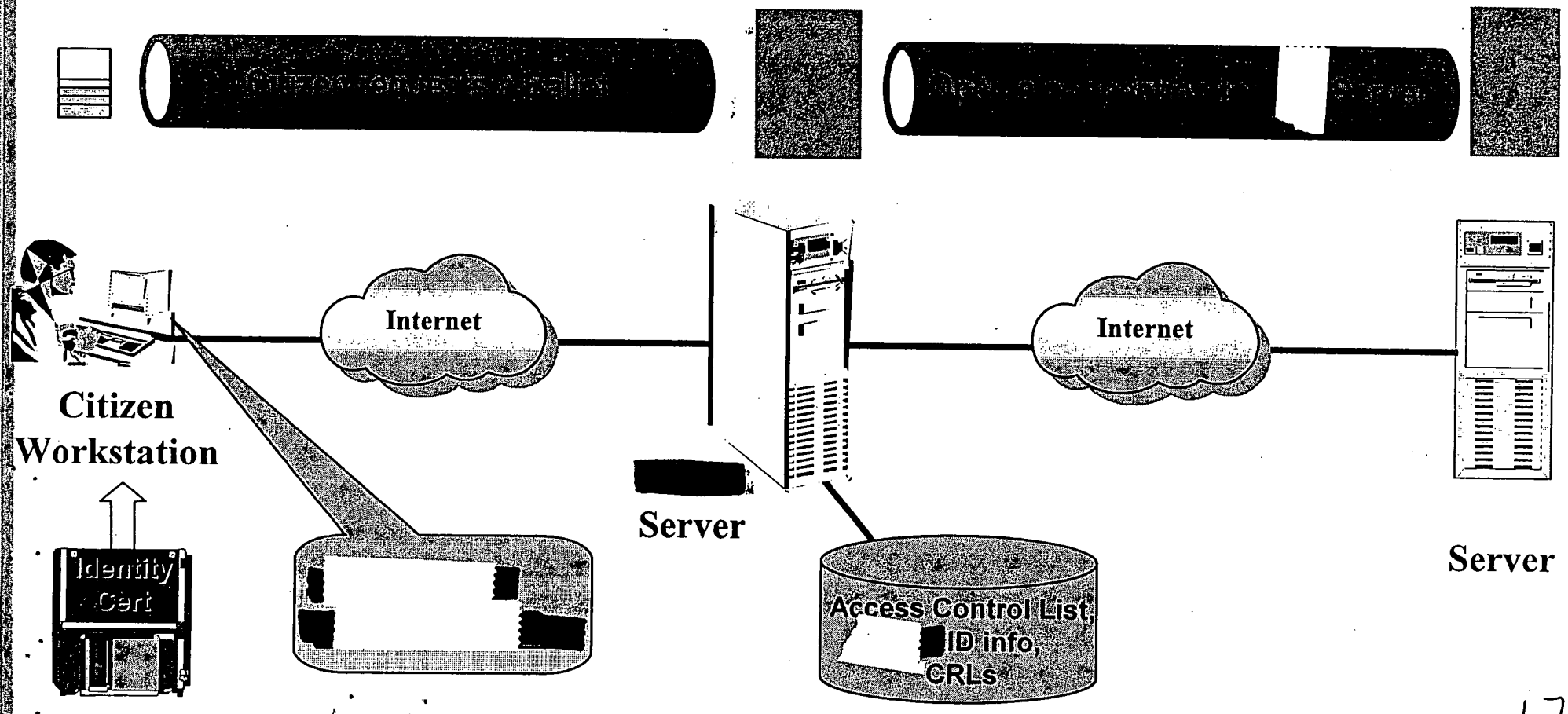
Blank Ballot Creation



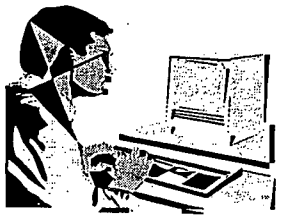
Blank Ballot Loading



Blank Ballot Retrieval by Citizen



Executing the Ballot



Citizen Workstation

Blank Ballot Form
Election Questions
Specific Instructions
Oath (optional)

[redacted] Privacy Cert

[redacted] Signature

[redacted] Identity Cert

ID Tag
[redacted] ID & Ballot Type

Executed Ballot
Vote Selections
Oath Attested

Encryptor Function

Verify

Identity Cert

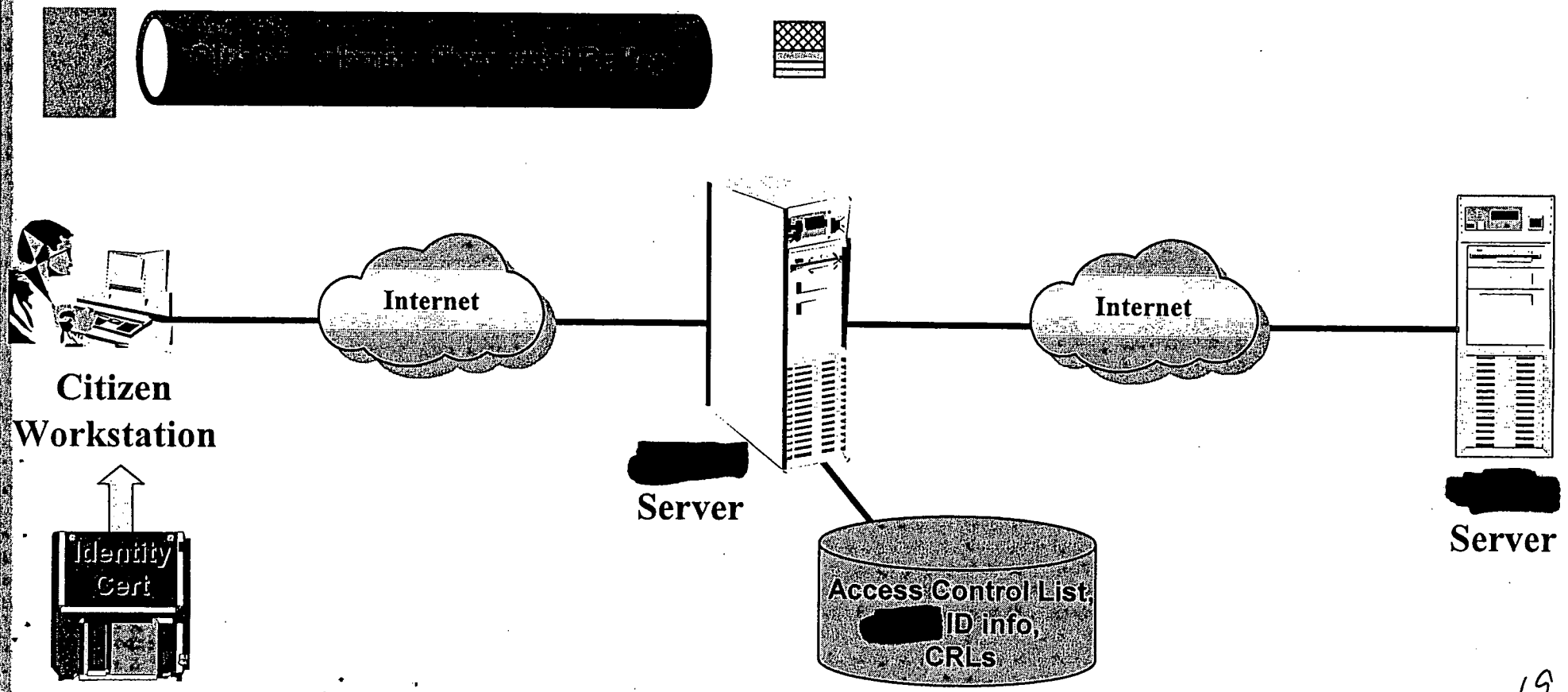
Encrypted Executed Ballot
Encrypted Data

ID Tag
[redacted] ID & Ballot Type

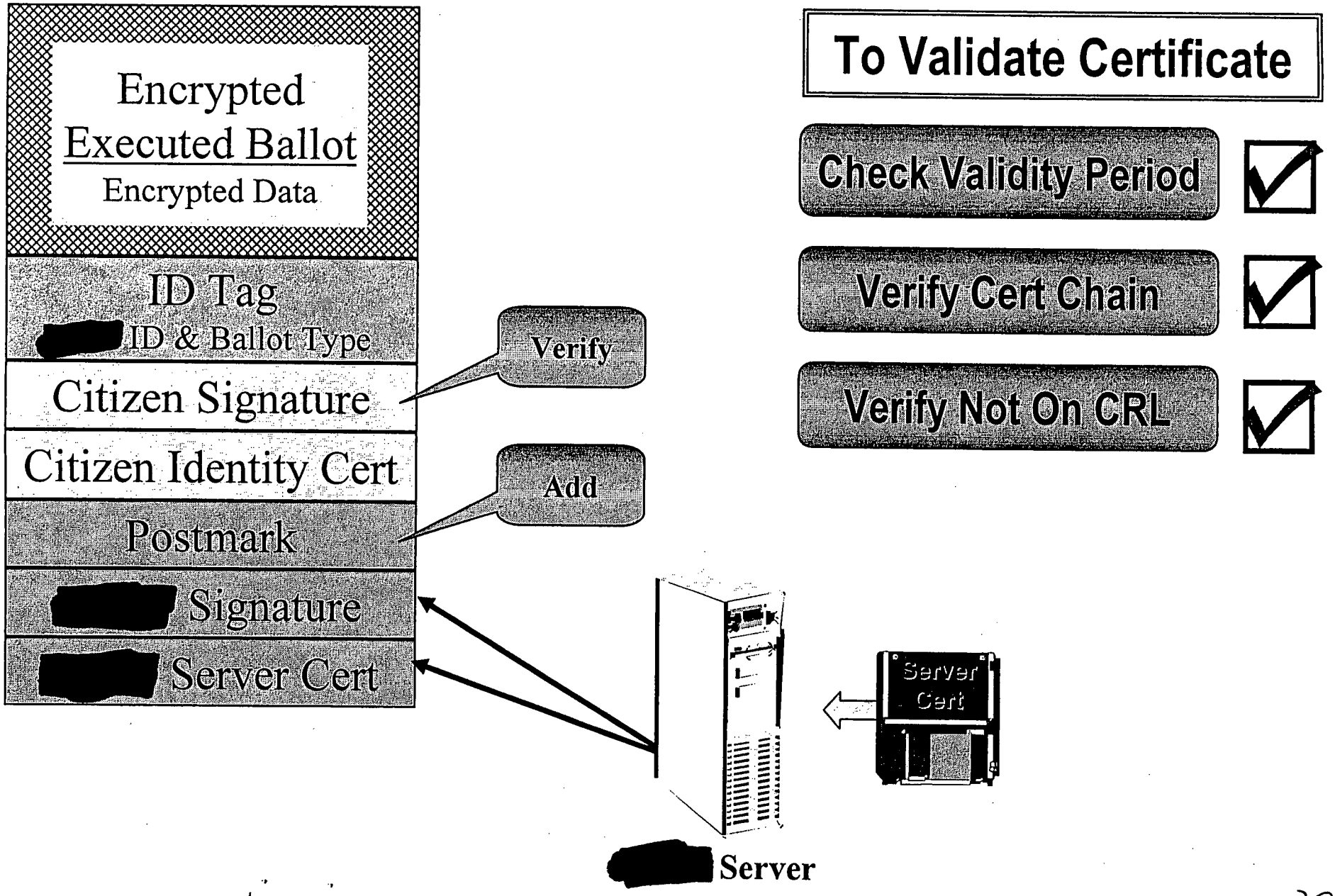
Citizen Signature

Citizen Identity Cert

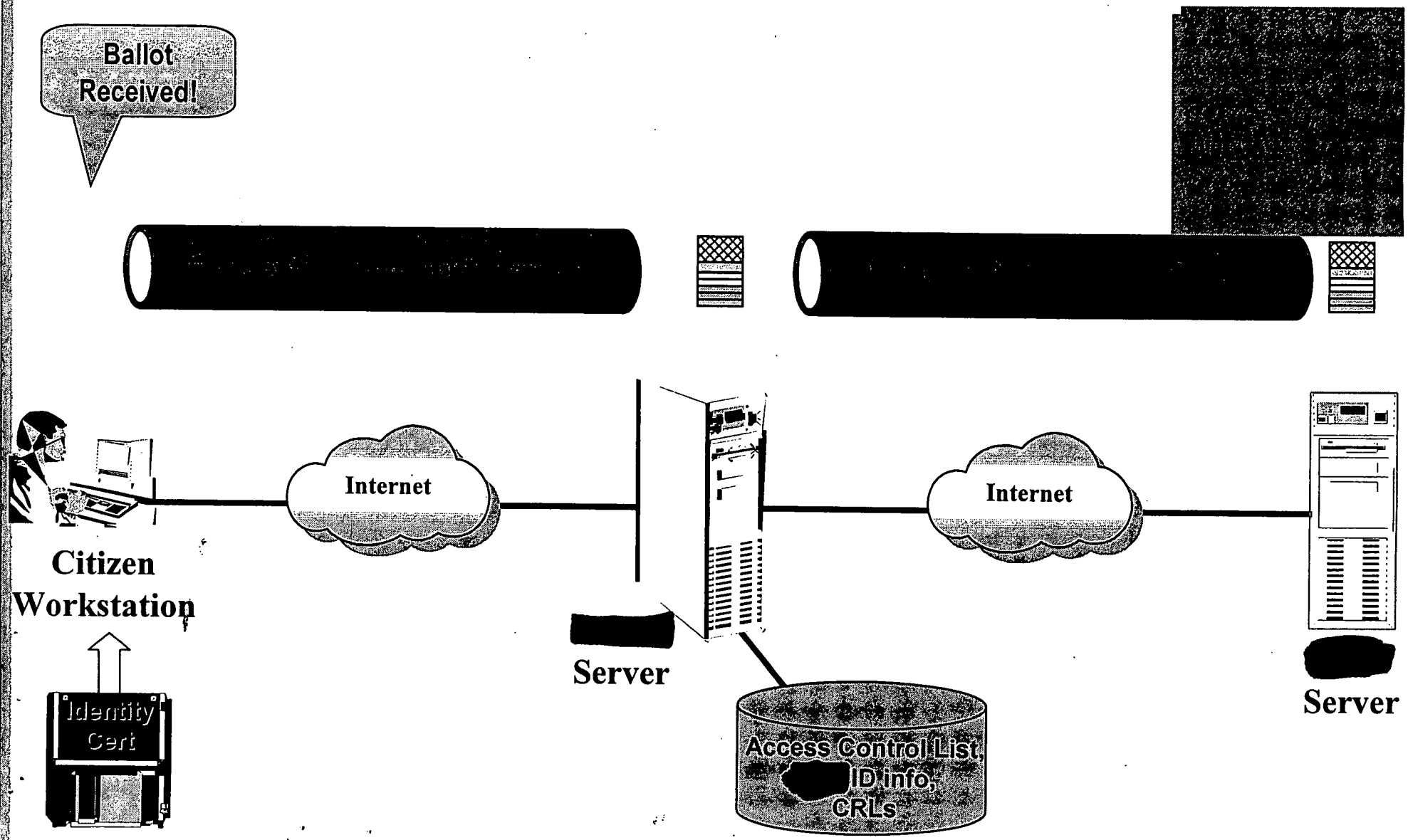
Executed Ballot Submission



Validating the Citizen



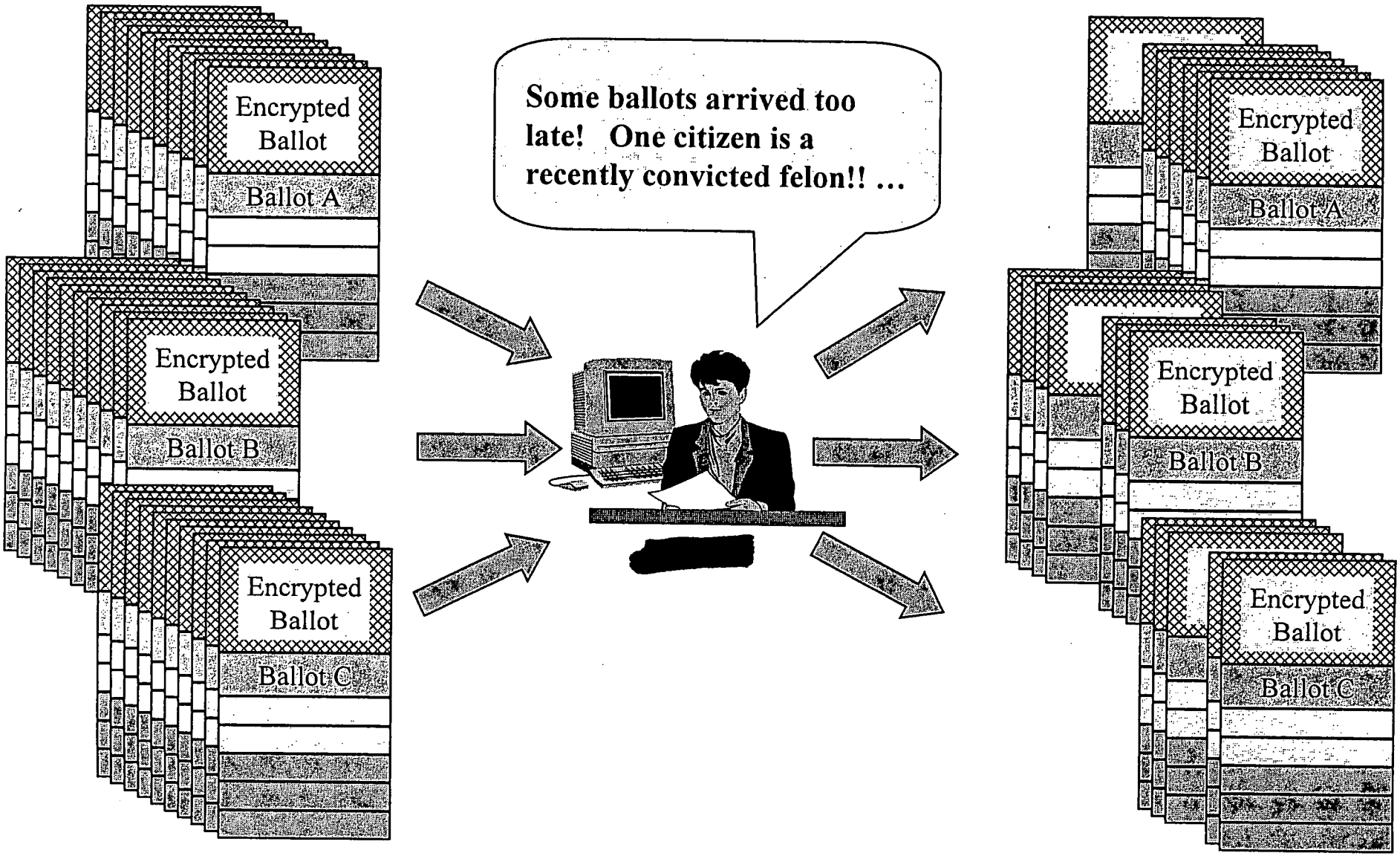
Executed Ballot Forwarding



Post Election Ballot Processing

- **Ballot Reconciliation**
 - Votes may be invalidated for a variety of reasons
 (Late Arrival, Citizen recently became ineligible, etc.)
 - System generates voting statistics
- **Ballot Separation**
 - Ballots must be anonymous -> signatures removed
- **Ballot Decryption & Printing**
 - Printed output used for election tallying

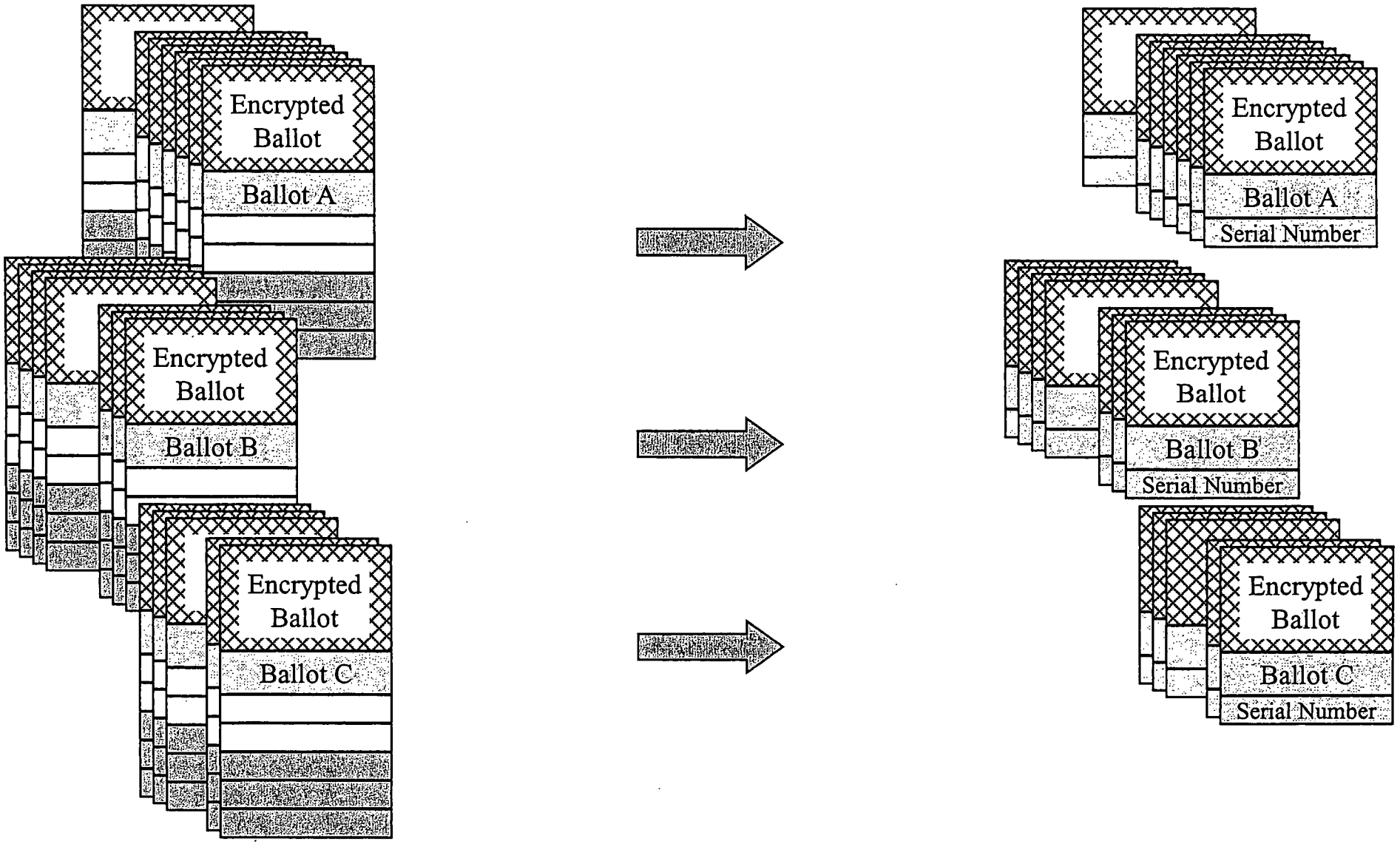
Ballot Reconciliation



All Ballots Received

Ballots to be Counted

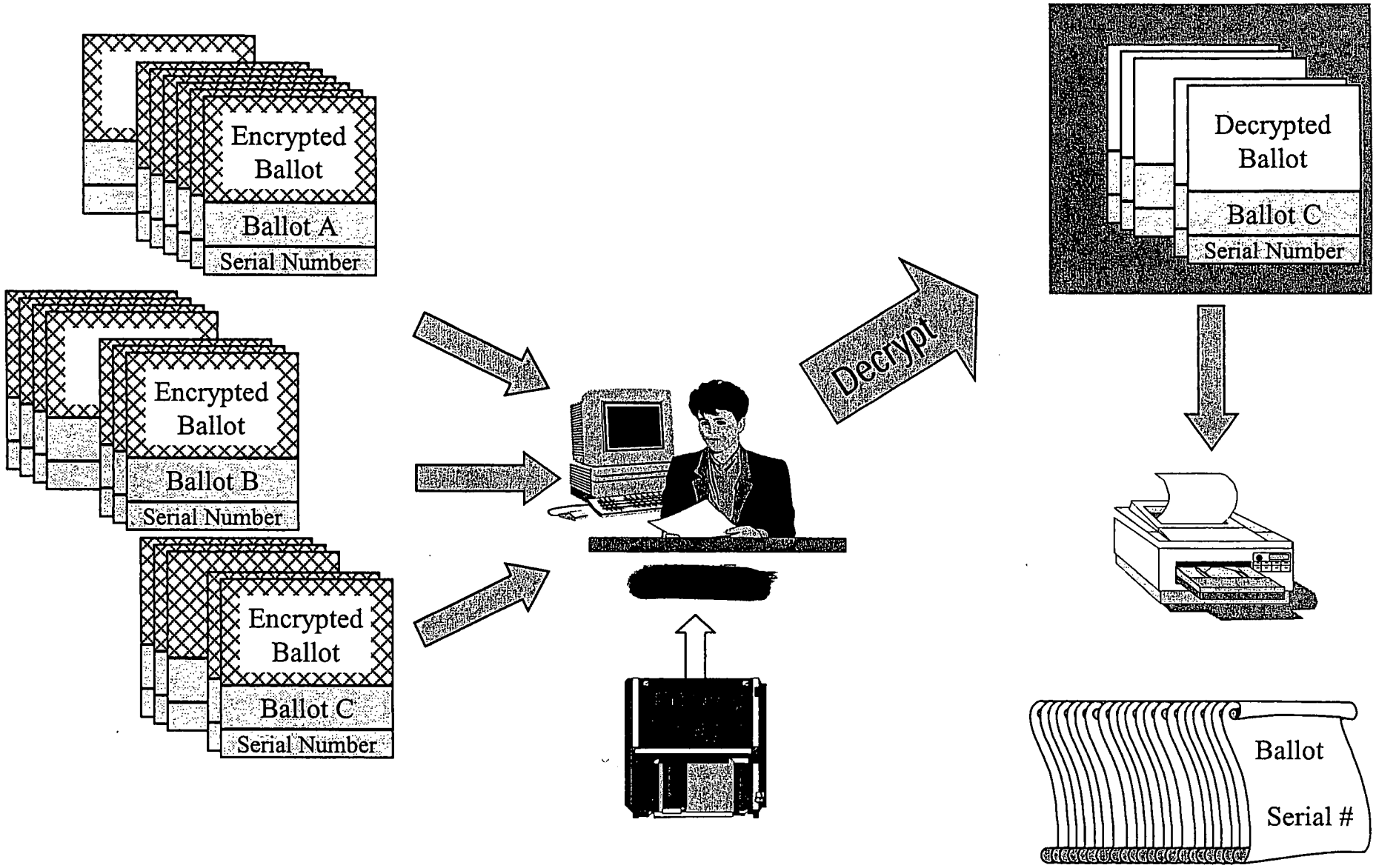
Ballot Separation



Ballots to be Counted

Anonymous Ballots

Ballot Decryption & Printing



Anonymous Ballots

Printed Ballots

Transmission Security

- Provides protection for connections [redacted]
- Secure Sockets Layer (SSLv3) Security
 - Most economical way to provide for transaction privacy
 - Strong mutual authentication for [redacted] comms
 - [redacted] more static and configuration controlled
 - Pre-placement of trusted Root and CA keys is achievable through admin functions

Transmission Security (cont'd)

- Secure Sockets Layer (SSLv3) Security (cont'd)
 - One-way authentication of Citizens [redacted]
 - Provides for a Pilot Access Control Mechanism
 - [redacted]

Transmission Security

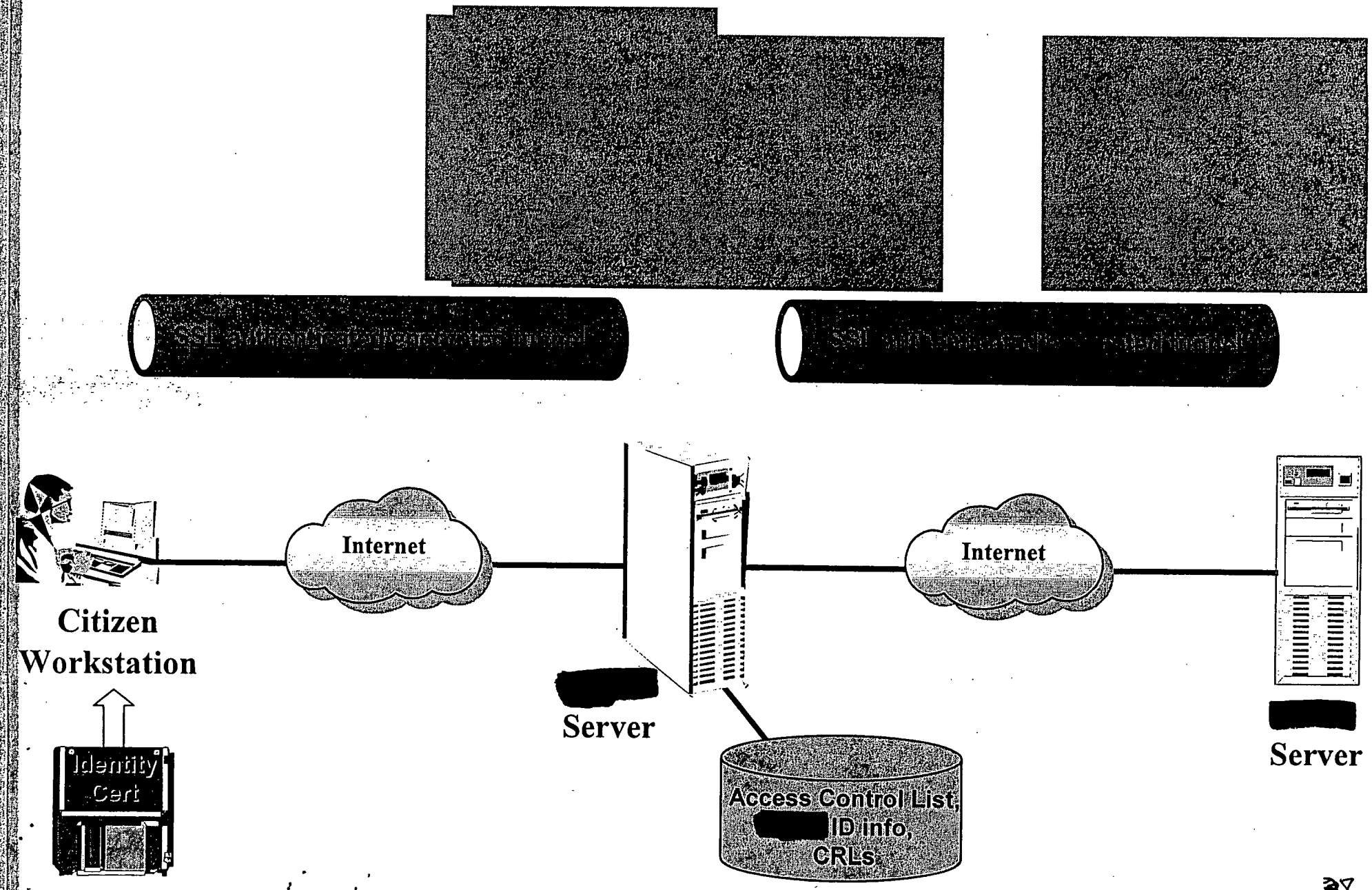
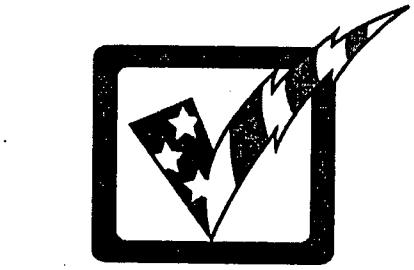


EXHIBIT C

51 page document prepared prior to November 2000, entitled "System Overview"

[redacted] System Overview

[redacted]



[redacted]

Document Overview

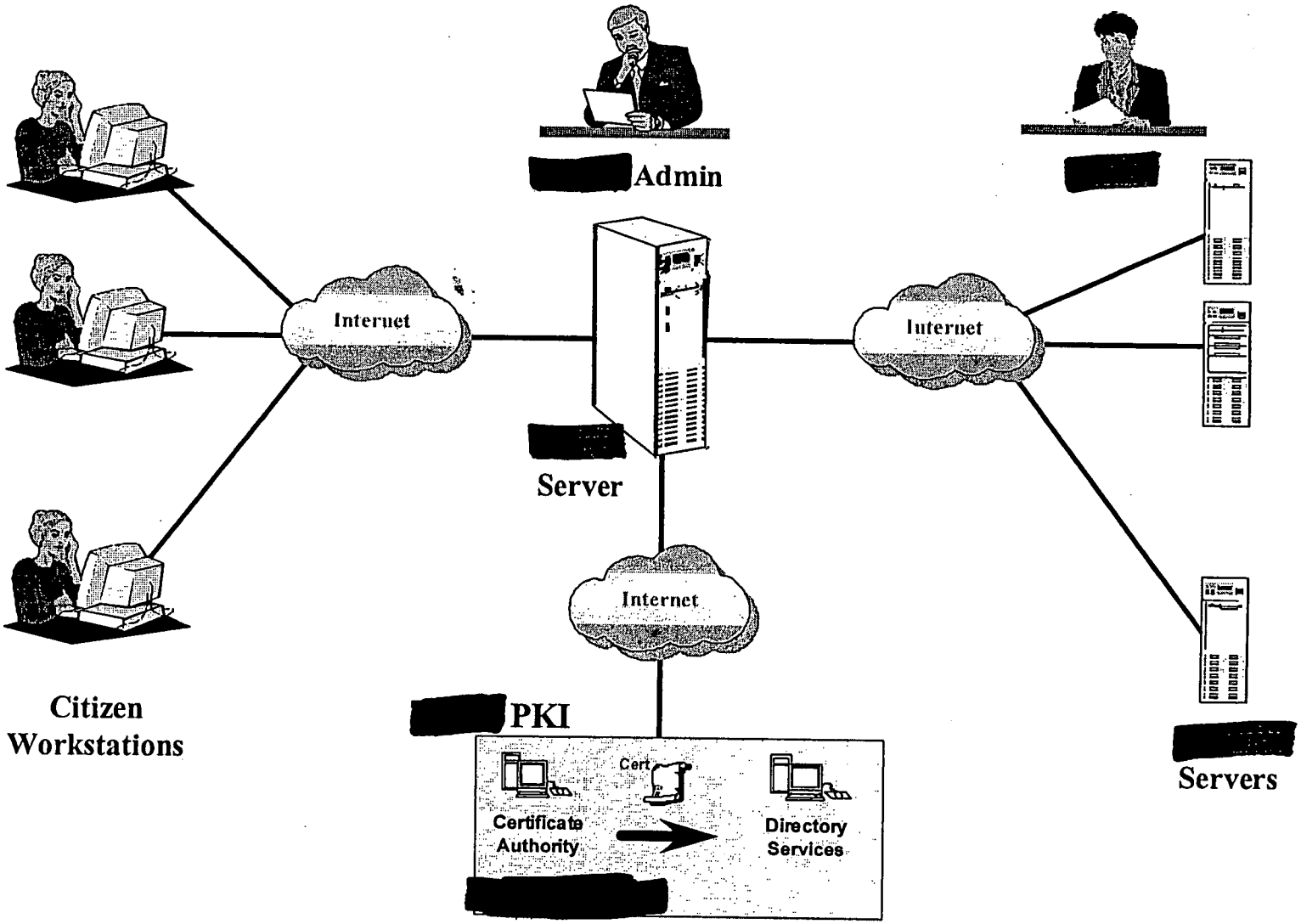
Document Contents

- [redacted]Architectural Views
- [redacted] System Components
- Object Walkthroughs
 - Login
 - [redacted]
 - E-Ballot
 - Citizen Status
- Additional Security Measures
 - System Roles
 - Personnel Access Control
 - Transmission Security
 - Cryptographic Security Services

[redacted]

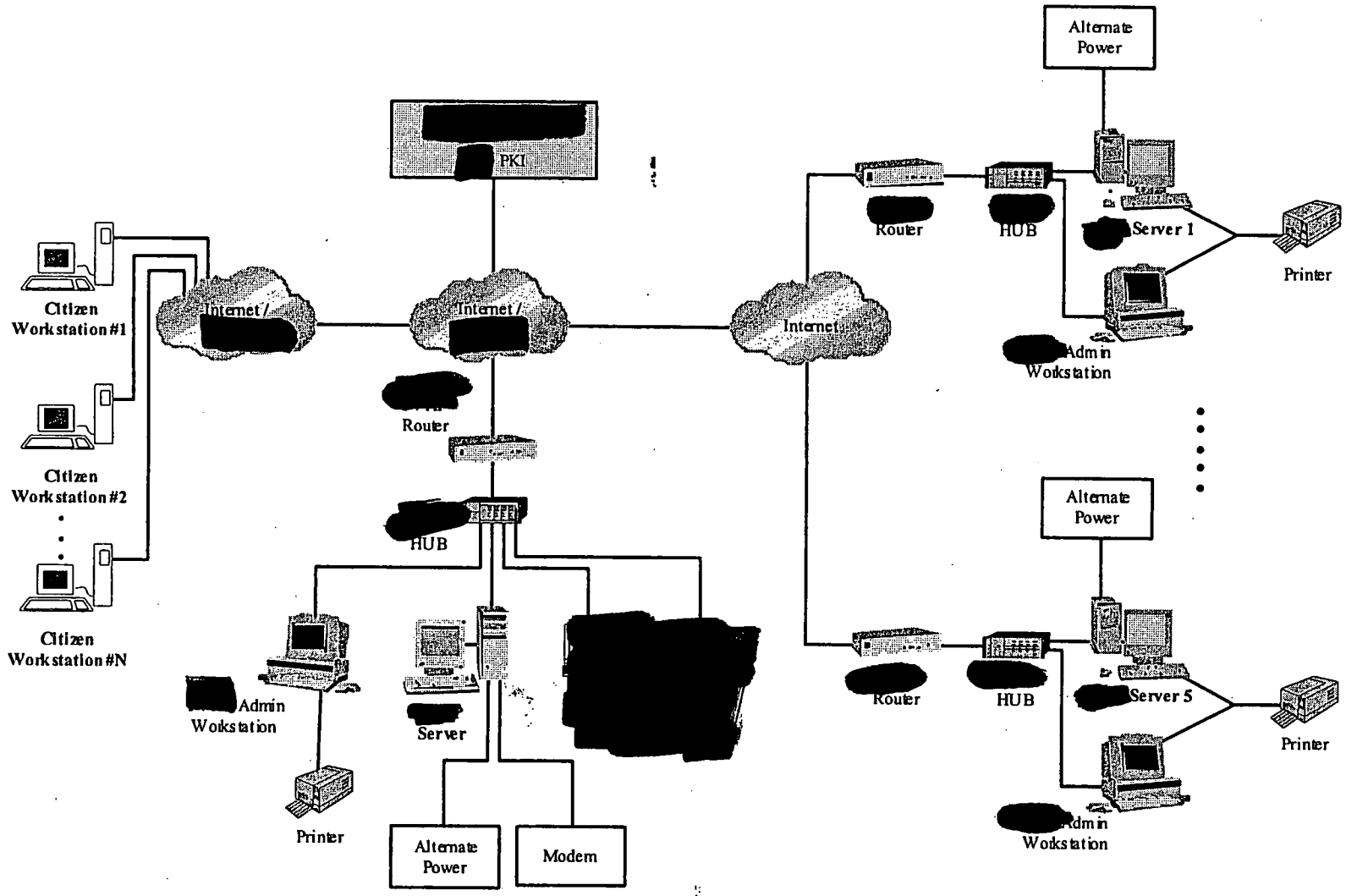
[redacted] Architecural Views

[redacted] System Architecture



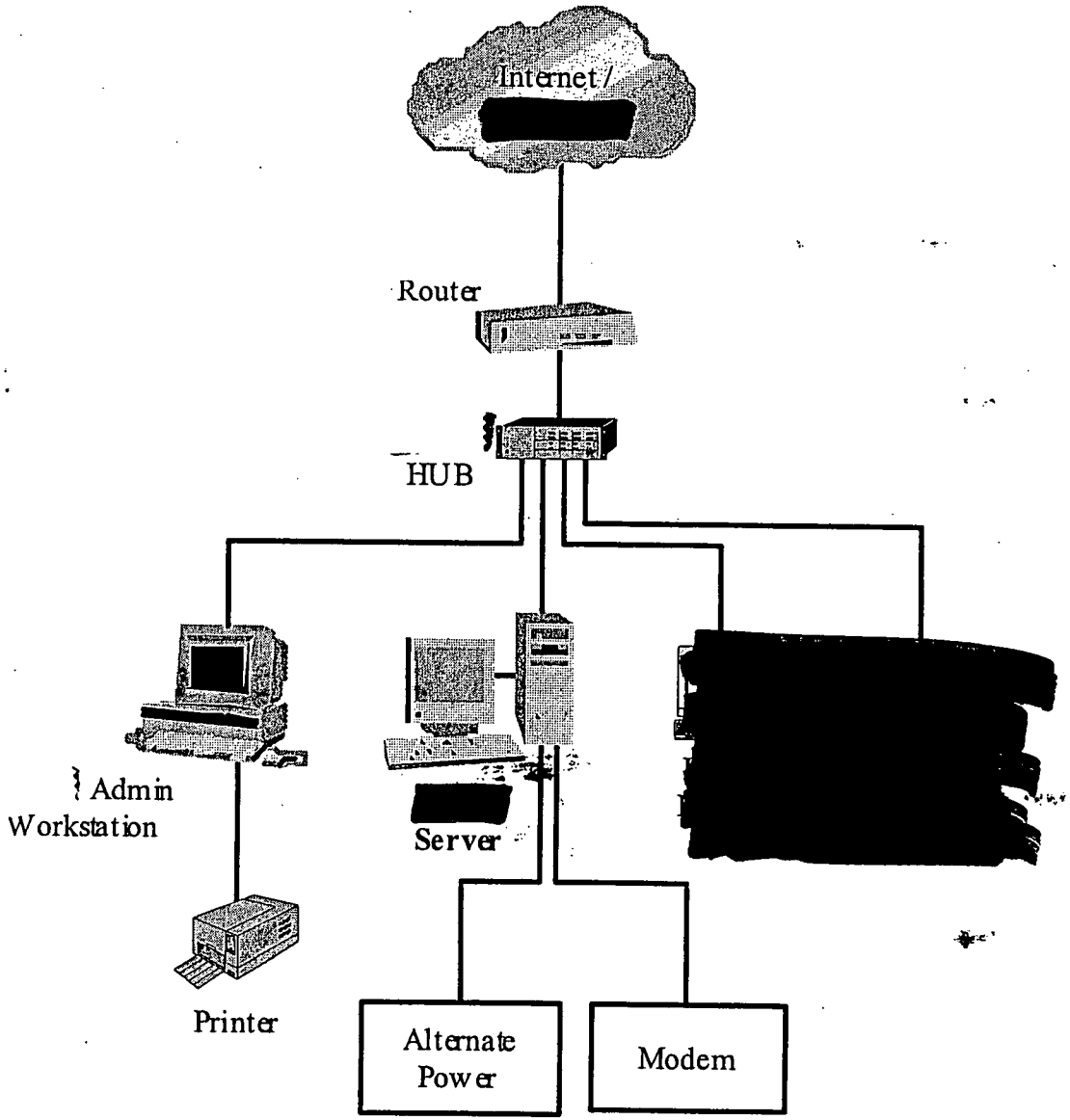
[redacted]

[redacted] System Architecture



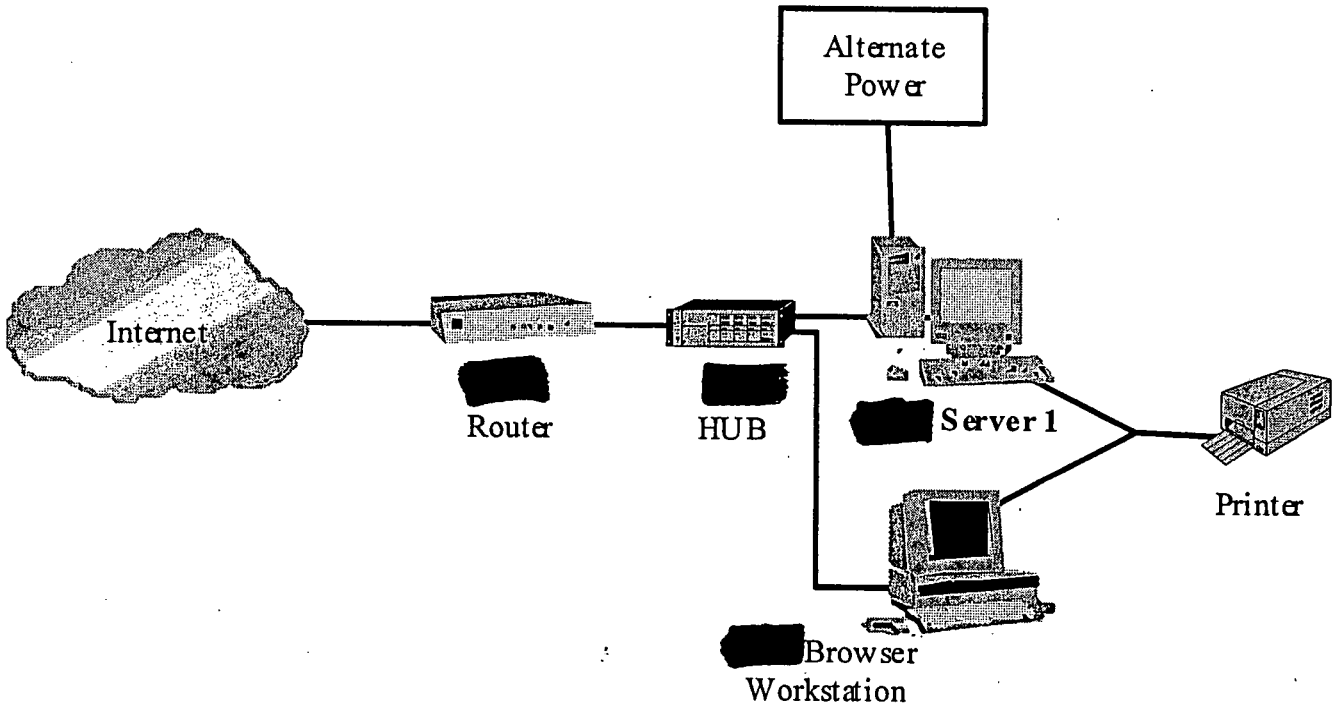
[redacted]

[redacted] Site Architecture



[redacted]

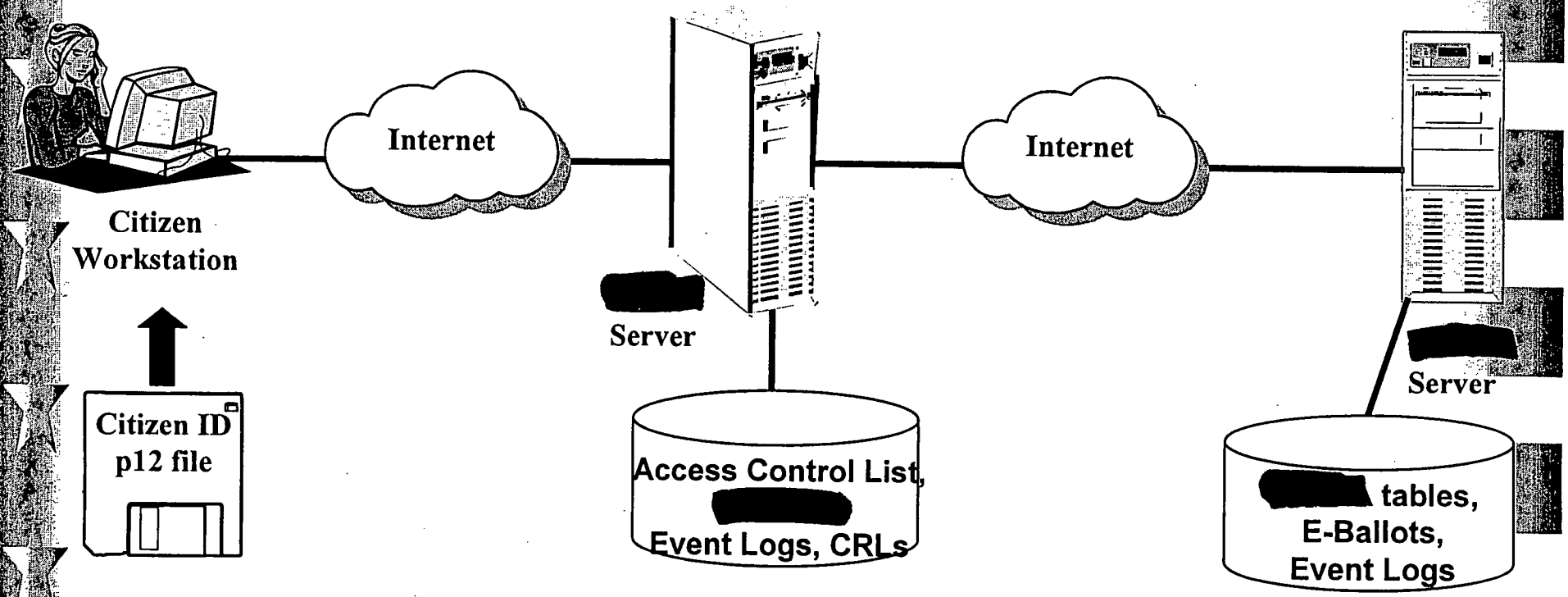
[redacted] Site Architecture



[redacted]

Certificate-Based Citizen Login Walkthrough

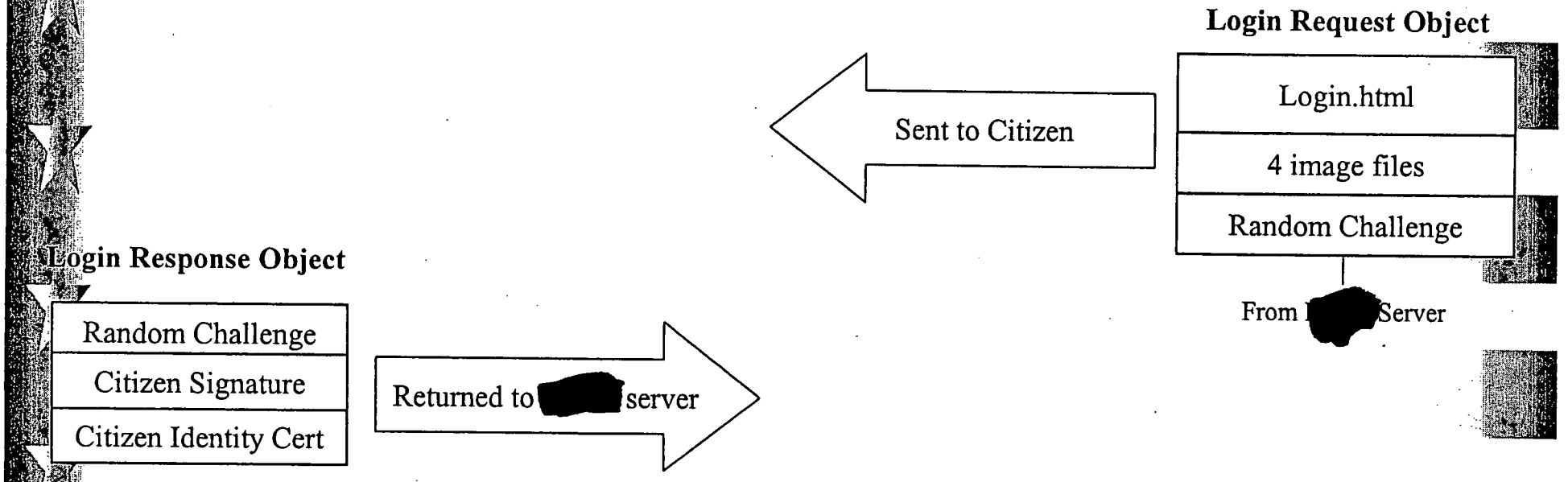
Citizen accesses [redacted] System



- Citizen types in web address of [redacted] server - [redacted]
- SSL3 connection is initiated - encrypted session begins
- [redacted] server generates Login Request object
 - Object includes one-time random number
- [redacted] stores random number for session verification

[redacted]

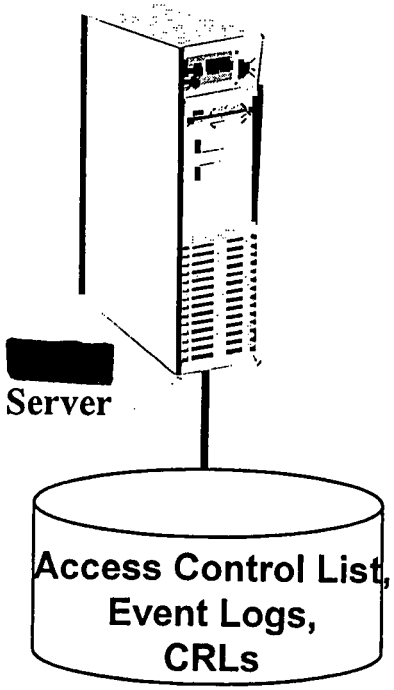
Login Request and Response



- **Plug-in invoked for Login Request object, Login page displayed**
 - Citizen is prompted for and inserts p12 floppy
- **Login Response object is constructed using contents of Login Request**
- **Response is signed using Citizen ID private key, cert attached to PKCS#7 object**
- **Object is sent to [redacted] server**

[redacted]

Citizen Login Response validated



Login Response Object

Login Html
4 image files
Random Challenge
Citizen Signature
Citizen Identity Cert

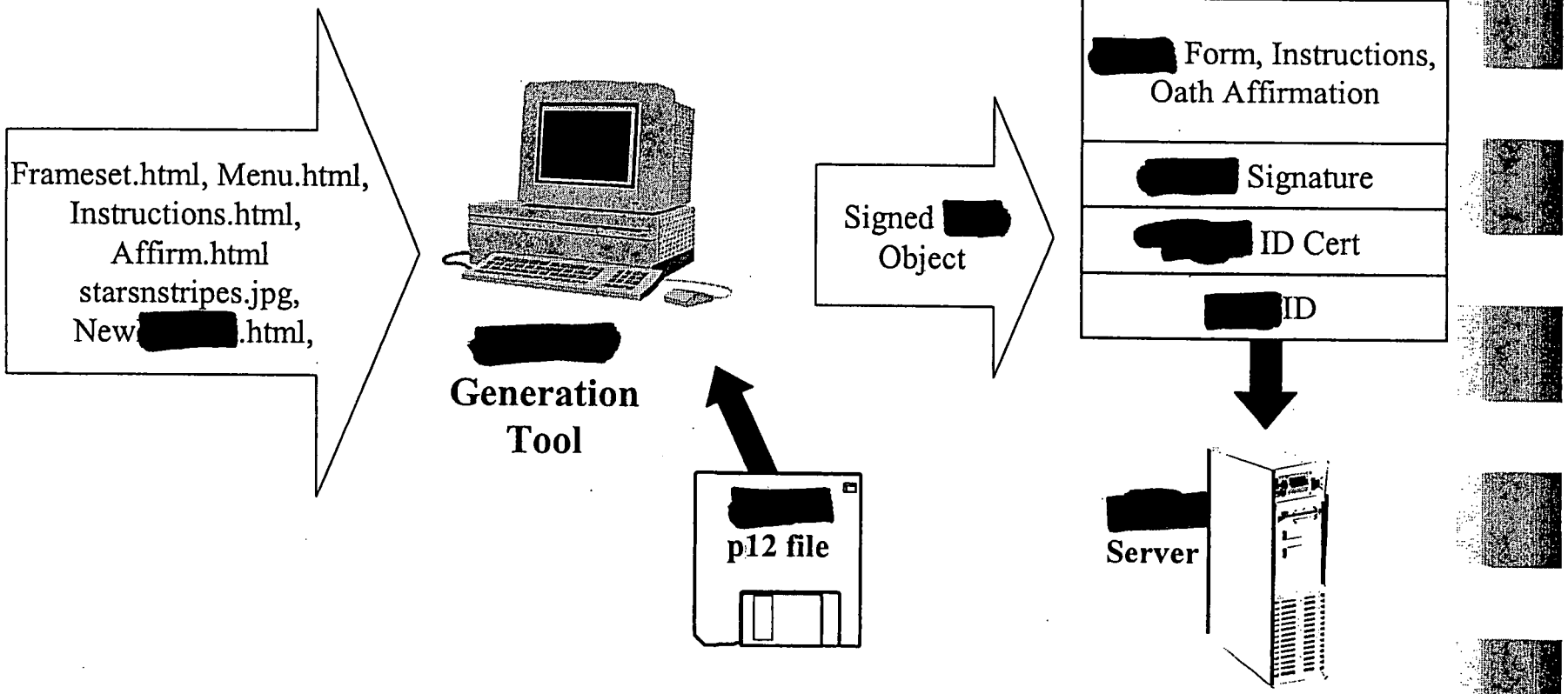
- **[redacted] server verifies Citizen signature, validates cert chain, and performs CRL check**
- **[redacted] server verifies session**
 - Random number from Login Response is compared with previously retained random
- **Assuming all checks are positive, the [redacted] server associates the session with the Citizen CN and provides the Citizen with the [redacted] Services page**

[redacted]

Walkthrough

Creation and Loading

[redacted] generation



- [redacted]
 - [redacted] generated by system developer, signed with [redacted] certificate, and copied onto [redacted] server
 - [redacted]

[redacted]

[redacted]

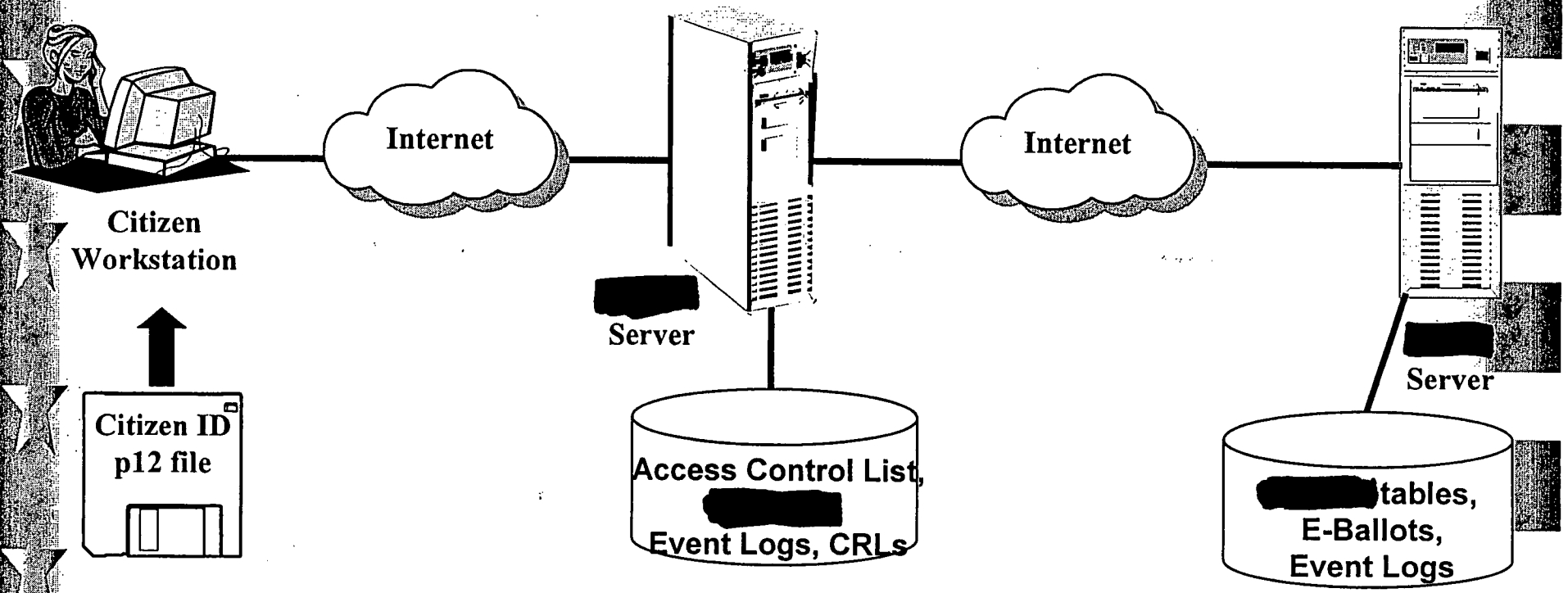
[redacted]

Walkthrough

[redacted]**Request & Submission**

[redacted]

Citizen requests [redacted]



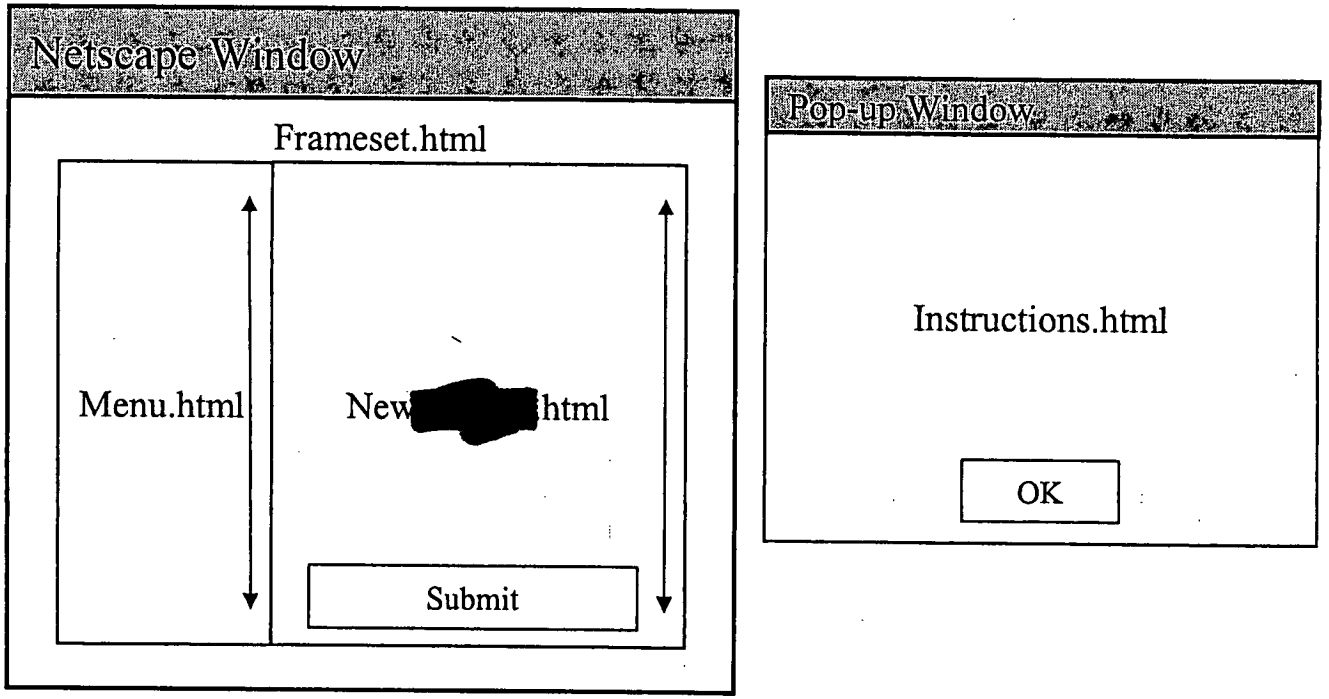
- **Citizen login to [redacted] server**
 - Plug-in invoked for cert-based login, citizen inserts p12 floppy
- **Requests to Register [redacted]**
- **Coonection opened to appropriate [redacted] server**
- **[redacted] server provides the apropriate [redacted] object**

[redacted]

[redacted] received



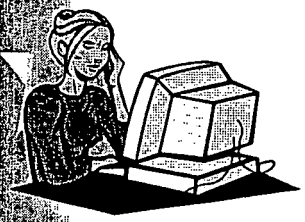
Citizen Workstation



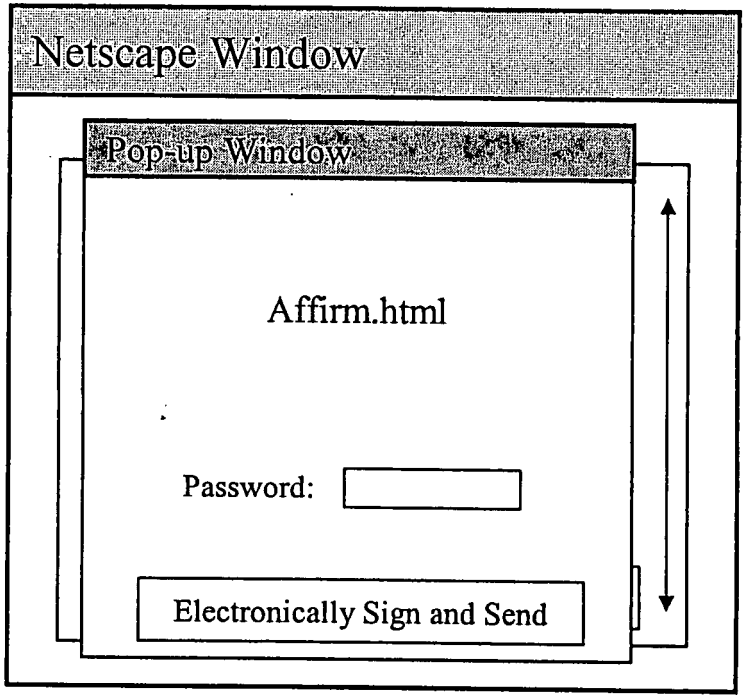
- **Plug-in invoked again for Blank [redacted] object**
- **[redacted] signature verified, message object parsed, Frameset, Menu, and [redacted] form are displayed - along with Instructions Pop-up window**
- **Citizen types personal information, clicks on "Submit" button**
 - If mandatory fields are missing, pop-up window informs citizen and enforces their return to the [redacted] form

[redacted]

[redacted] selections affirmed



Citizen Workstation



- Once Submit is selected, plug-in displays the affirmation choices made by the citizen at the bottom of the [redacted], along with any required State oath
- Citizen is also asked to insert their p12 floppy and enter their certificate password

[redacted]

Completed [redacted] construction

Blank [redacted] Object

[redacted] Form, Instructions, Oath Affirmation
[redacted] Signature
[redacted] ID Cert
[redacted] ID



Citizen Inputs

Completed [redacted] Object

Completed [redacted] Form, Affirmation & Oath Text
[redacted] ID
Citizen Signature
Citizen ID Cert

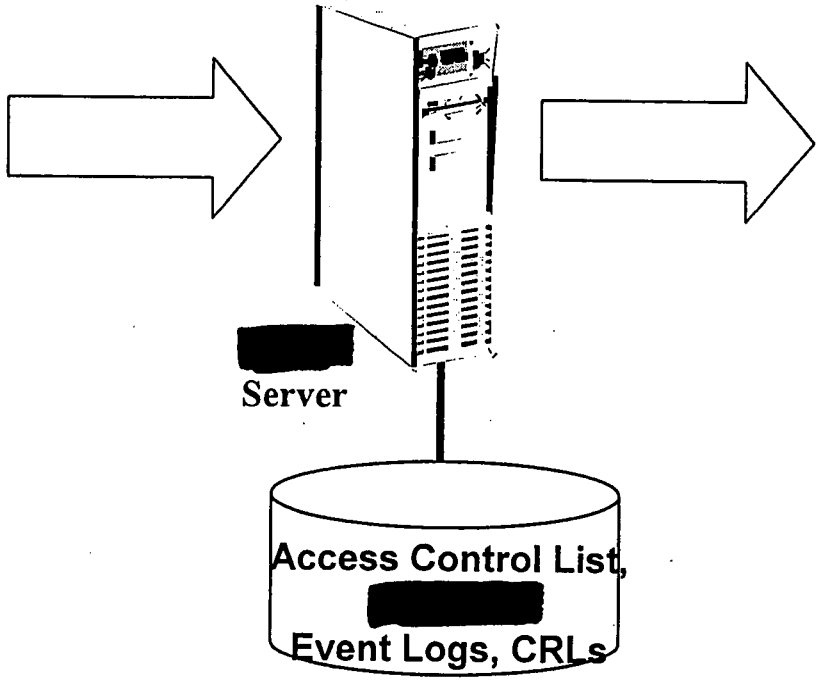
- **Citizen inputs are combined with [redacted] form**
- **[redacted] ID is copied to new object**
- **Plug-in is invoked again for signing the completed [redacted]**

[redacted]

[redacted] postmarked & validated

Completed [redacted] Object

Completed [redacted] Form, Affirmation & Oath Text
[redacted] ID
Citizen Signature
Citizen ID Cert



Validated [redacted] Object

Completed [redacted] Form, Affirmation & Oath Text
[redacted] ID
Citizen Signature
Citizen ID Cert
Postmark
[redacted] Signature
[redacted] ID Cert

- **[redacted] server attaches postmark, verifies Citizen signature, validates cert chain, does CRL check, signs object - forwards to [redacted] server indicated in [redacted] ID tag**
- **[redacted] verifies [redacted] Citizen signatures (for integrity), provides response to [redacted]**
- **[redacted] erases all data files for Validated [redacted] and provides response to Citizen**
- **Plug-in erases all data files for Blank and Completed [redacted]**

[redacted]

[redacted]

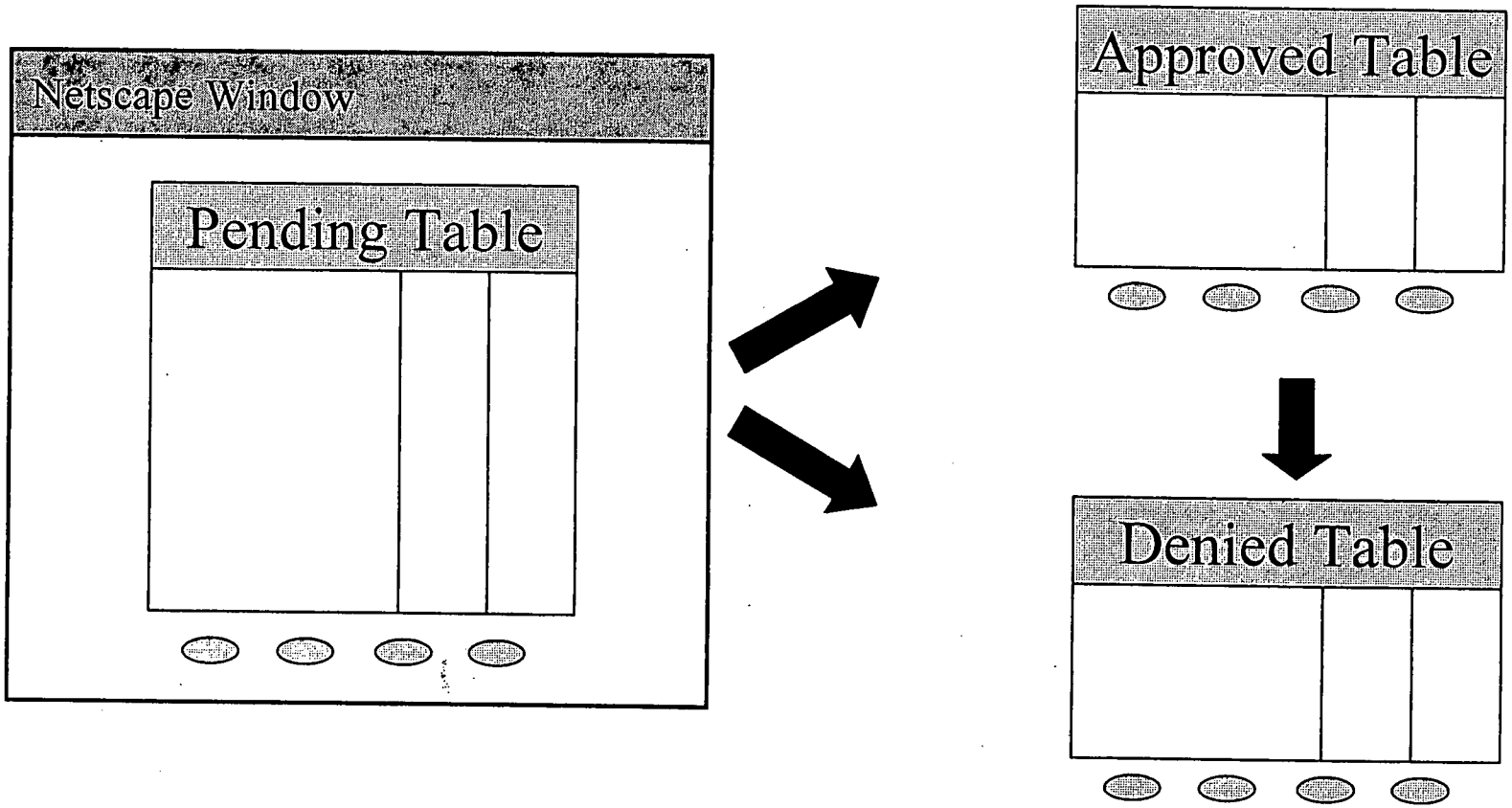
[redacted]

Walkthrough

[redacted] Processing by [redacted] Personnel

[redacted]

Processing of [redacted]



- **All received [redacted] are intially placed in the Pending Table**
- **[redacted] personnel approve or deny requests to vote [redacted] based on the citizen information provided within the form - but [redacted] objects NEVER change**
- [redacted]
 - Signatures are rechecked each time [redacted] is viewed

[redacted]

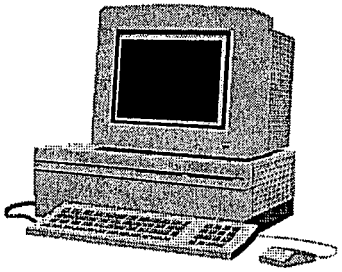
E-Ballot Walkthrough

E-Ballot Creation and Loading

E-Ballot generation

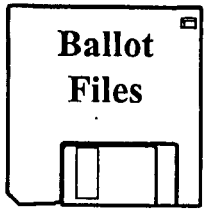


Human Inputs



Ballot Generation Tool

4 HTML Files

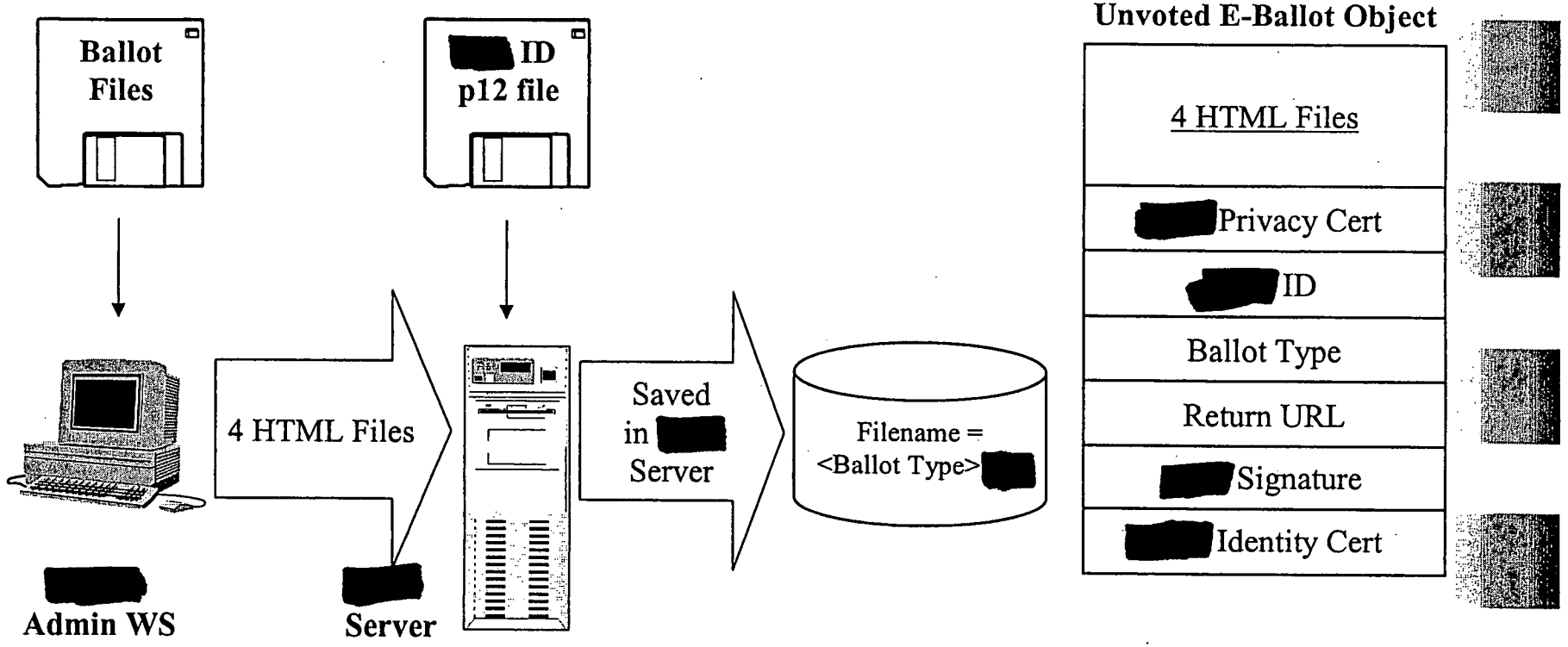


Note: One Ballot per floppy

- **Ballot contents specified by [redacted] personnel, 4 files downloaded and saved to floppy**
 - EBallot_Frameset.html (contents obvious)
 - EBallot_ Left.html contains index for the E-Ballot
 - EBallot_ Right.html contains the bulk of the E-Ballot object, including most javascript needed by plug-in
 - EBallot_ Affirm.html contains an Oath (optional), affirmation statement, and javascript needed by plug-in for the "Electronically Sign and Send" button

[redacted]

Load E-Ballot



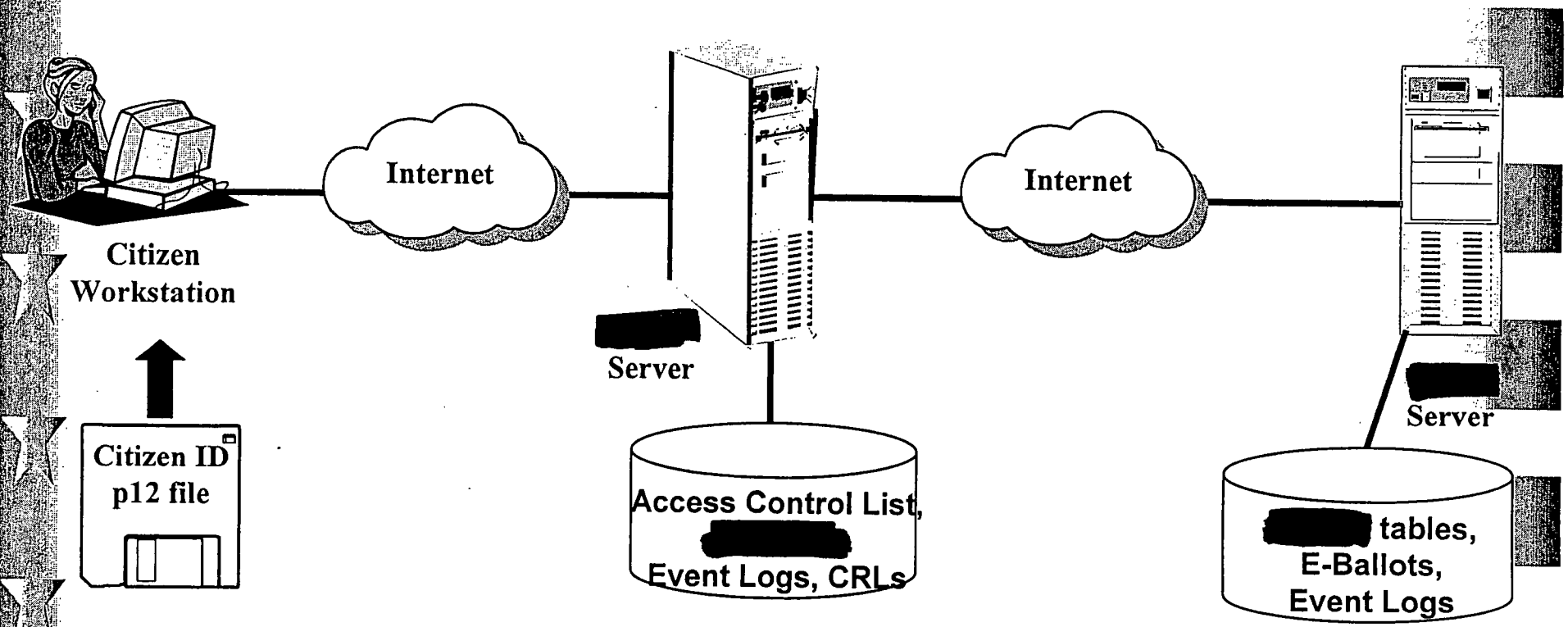
- **Privacy Cert & Ballot Type are preloaded by the [redacted], [redacted] ID & Return URL are hard coded at the [redacted] server**
 - Note: These pieces are added to the object before signing
- **Object signed with [redacted] ID private key, cert is included in the PKCS#7 object**

[redacted]

E-Ballot Walkthrough

Unvoted E-Ballot Request & Voted E-Ballot Submission

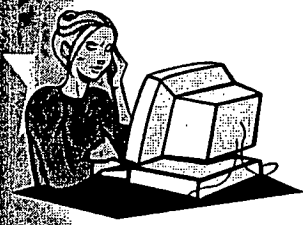
Citizen requests Unvoted E-Ballot



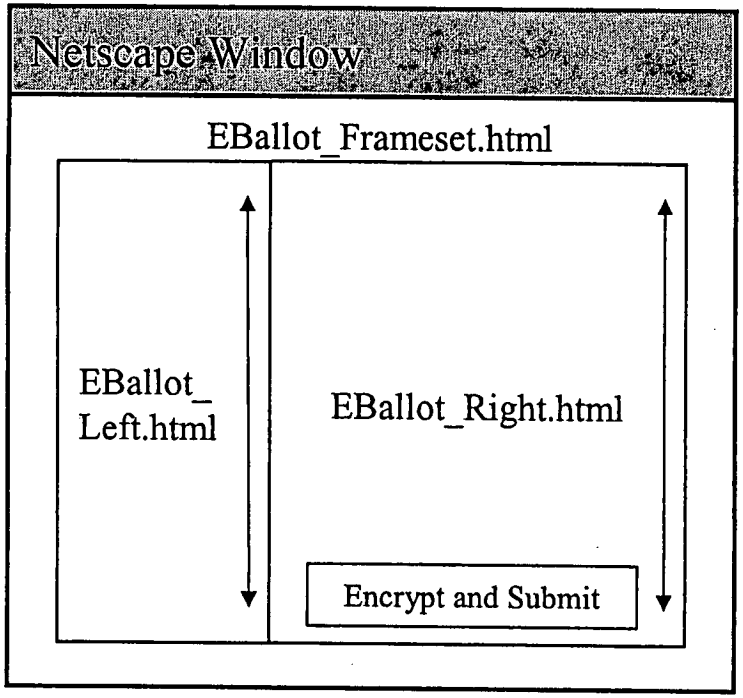
- **Citizen login to [redacted] server**
 - Plug-in invoked for cert-based login, citizen inserts p12 floppy
- **Requests to Vote, [redacted]**
- **Request forwarded to appropriate [redacted] server with Citizen CN**
- **Various tests performed, Unvoted E-Ballot object provided, [redacted] server relays**

[redacted]

Unvoted E-Ballot received



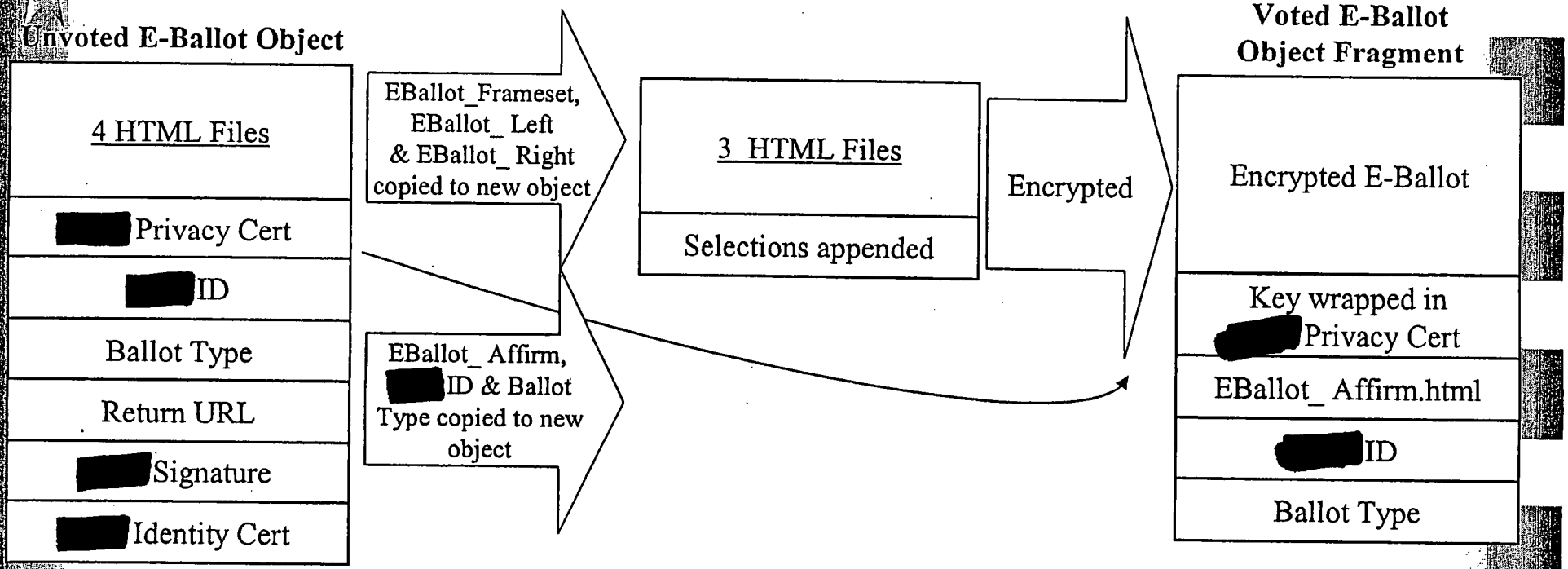
Citizen Workstation



- Plug-in invoked again for Unvoted E-Ballot object
- [redacted] signature verified, message object parsed, EBallot_ Frameset, EBallot_ Left, and EBallot_ Right displayed
- Citizen makes all selections, clicks on "Encrypt and Submit" button

[redacted]

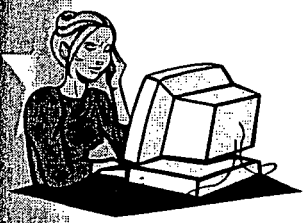
Voted E-Ballot construction begins



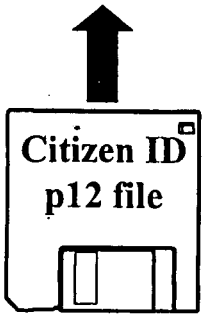
- **Voted E-Ballot construction begins with copying EBallot_ Frameset.html, EBallot_ Left.html and EBallot_ Right.html to an object fragment and appending the citizen's selections**
- **Object fragment is encrypted using [redacted] privacy cert**
 - Key created, object encrypted, key wrapped with privacy cert and included in the new PKCS#7 object
- **EBallot_ Affirm.html, [redacted] ID, Ballot Type are then appended to the object fragment**

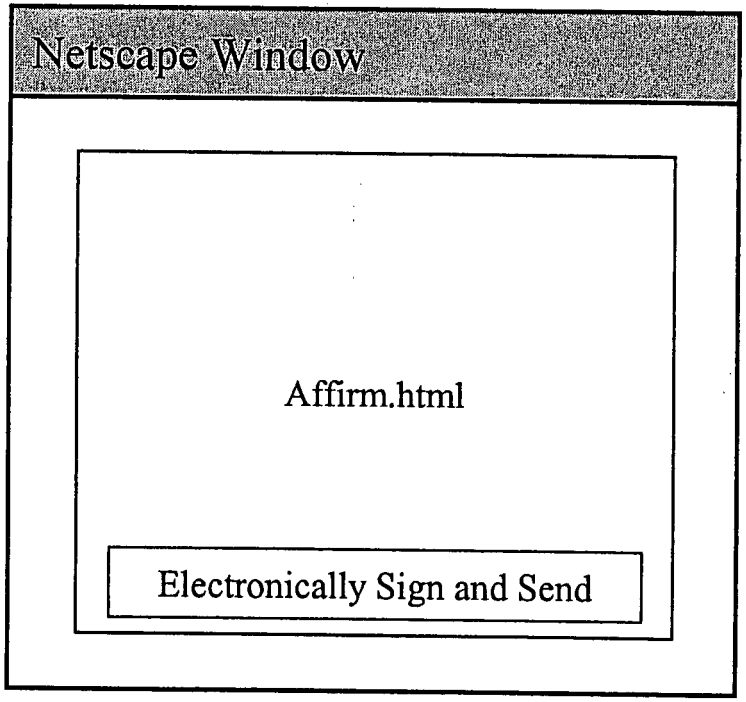
[redacted]

Oath/Affirmation - Voted E-Ballot completed



Citizen Workstation





Voted E-Ballot Object

Encrypted E-Ballot
Key wrapped in [redacted] Privacy Cert
EBallot_ Affirm.html
[redacted] ID
Ballot Type
Citizen Signature
Citizen Identity Cert

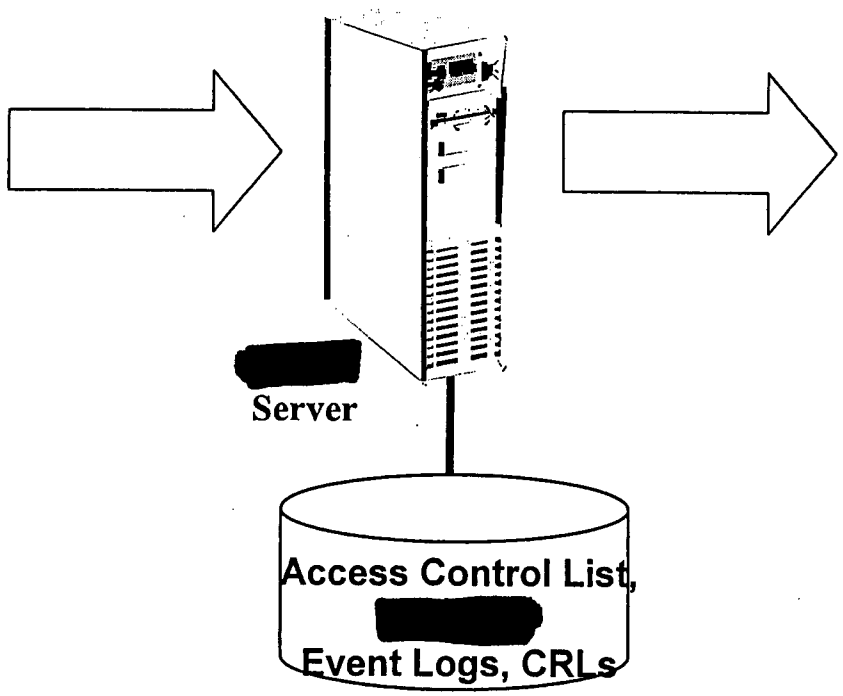
- **Immediately following previous steps, plug-in displays EBallot_ Affirm.html**
 - Contains [redacted] Oath [redacted] requests Citizen cert and password
- **Citizen inserts p12 floppy and selects "Electronically Sign and Send" button**
- **Object fragment is signed using Citizen ID private key, cert attached to larger PKCS#7 object**
- **Voted E-Ballot object is submitted to [redacted] server using Return URL from Unvoted E-Ballot**

[redacted]

Voted E-Ballot postmarked & validated

Voted E-Ballot Object

Encrypted E-Ballot
Key wrapped in [redacted] Privacy Cert
Affirm.html
[redacted] ID
Ballot Type
Citizen Signature
Citizen Identity Cert



Validated E-Ballot Object

Encrypted E-Ballot
Key wrapped in [redacted] Privacy Cert
Affirm.html
[redacted] ID
Ballot Type
Citizen Signature
Citizen Identity Cert
Postmark
[redacted] Signature
[redacted] Identity Cert

- [redacted] server attaches postmark, verifies Citizen signature, validates cert chain, does CRL check, signs object - forwards to [redacted] server indicated in [redacted] ID tag
- [redacted] verifies [redacted] signatures (for integrity), provides response to [redacted]
- [redacted] erases all data files for Voted & Validated E-Ballot, provides response to Citizen
- Plug-in erases all data files for Unvoted & Voted E-Ballot

[redacted]

E-Ballot Walkthrough

Post Election E-Ballot Processing

E-Ballot Reconciliation

Validated E-Ballot Objects

Encrypted E-Ballot
Key wrapped in [redacted] Privacy Cert
Affirm.html
[redacted] ID
Ballot Type
Citizen Signature
Citizen Identity Cert
Postmark
[redacted] Signature
[redacted] Identity Cert

- **All Validated E-Ballots are stored in a permanent directory, objects are never deleted**
- **[redacted] personnel process piles of Validated E-Ballot objects**
- **"View Details" verifies both signatures (for integrity purposes)**
- **Reconciliation makes no changes to E-Ballot objects, just E-Ballot tables**

[redacted]

E-Ballot Separation

Validated E-Ballot Object

Encrypted E-Ballot
Key wrapped in [redacted] Privacy Cert
Affirm.html
[redacted] ID
Ballot Type
Citizen Signature
Citizen Identity Cert
Postmark
[redacted] Signature
[redacted] Identity Cert

Separated

Temp E-Ballot Object

Encrypted E-Ballot
Key wrapped in [redacted] Privacy Cert
[redacted] ID
Ballot Type

H4&fgy6s[redacted]

PCN assigned

Separated E-Ballot Object

Encrypted E-Ballot
Key wrapped in [redacted] Privacy Cert
[redacted] ID
Ballot Type

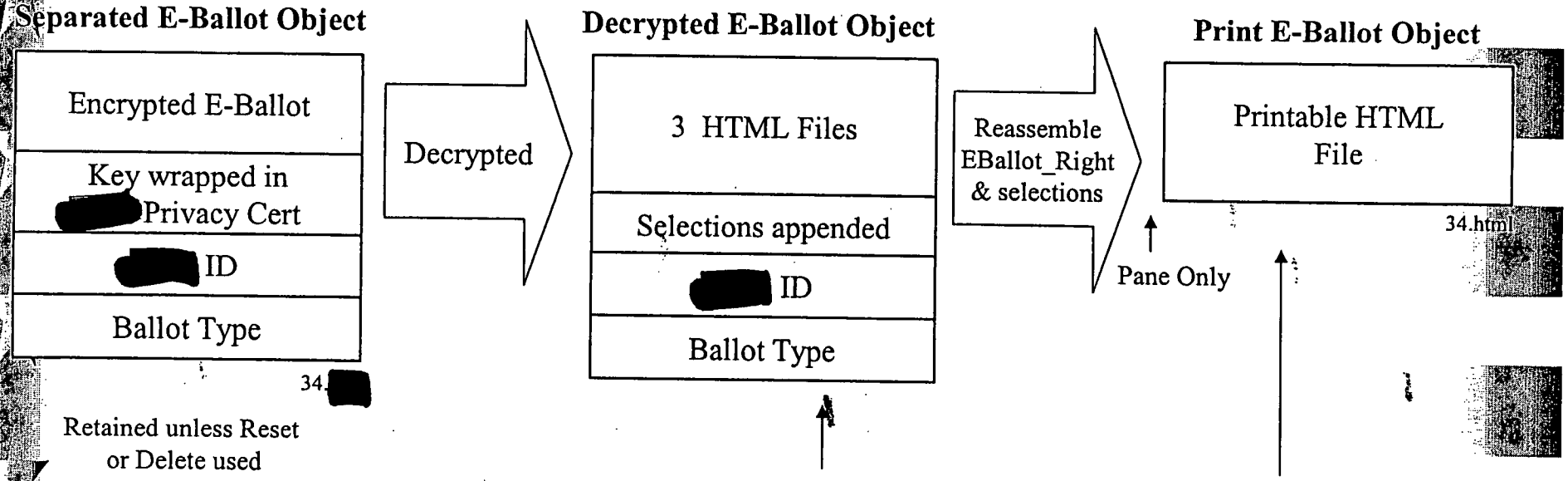
34[redacted]

Validated E-Ballot object retained in server

- **After reconciliation, E-Ballots are processed by type**
 - Separation strips signatures and postmark
 - Stripped files are placed in temp directory, files are named using random strings
- **Once all E-Ballots of a type are separated…**
 - E-Ballots are copied one by one (in alphabetical order) to a semi-permanent directory (Reset would erase these files)
 - Files are named based on PCN
 - Order of E-Ballots randomized
 - Temp E-Ballot objects are erased after each Type is processed

[redacted]

E-Ballot Printing

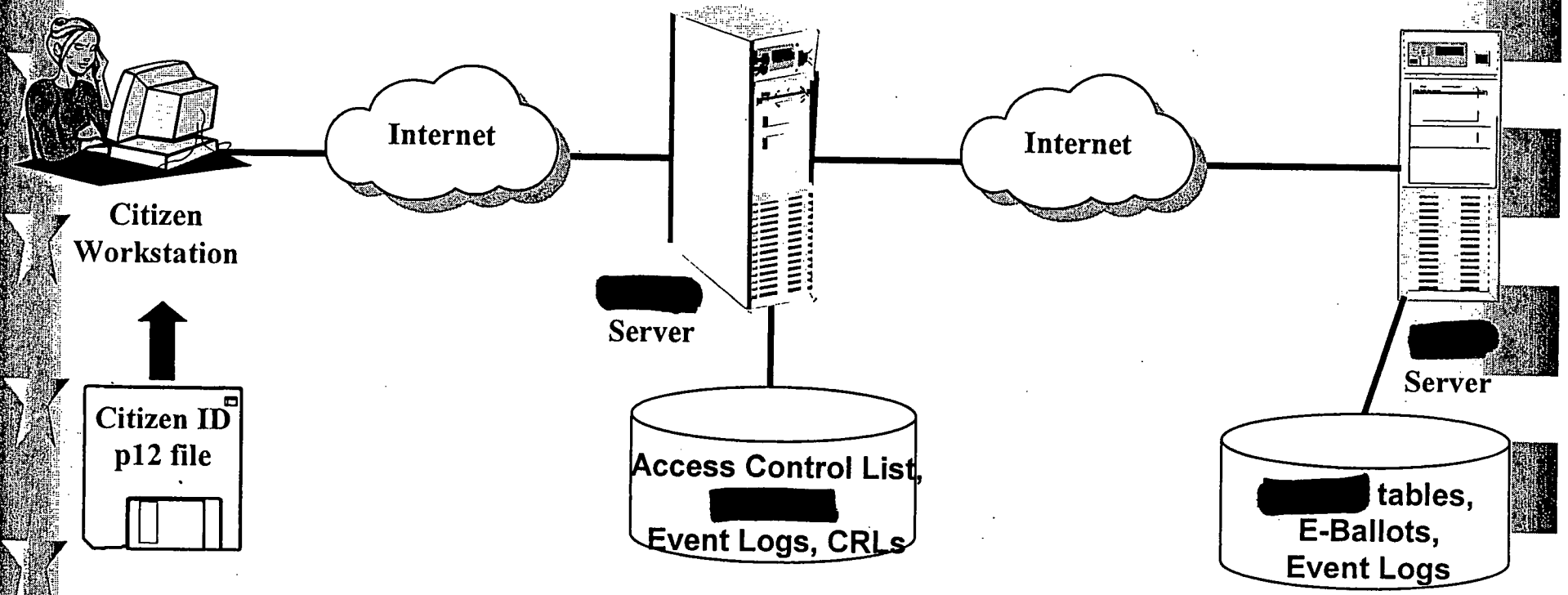


- [redacted] server decrypts E-Ballot, reassembles HTML into single printable file
- [redacted] server prints ballots one by one, with Ballot Type, PCN, page numbers, and date
- After each print is submitted, [redacted] erases Print E-Ballot objects
 - Note: Separated E-Ballots are retained for potential reprint

[redacted]

Citizen Status Walkthrough

Citizen requests status



- **Citizen login to [redacted] server**
 - Plug-in invoked for cert-based login, citizen inserts p12 floppy
- **Citizen requests Status, [redacted]**
- **Request forwarded to appropriate [redacted] server with Citizen CN - *No Objects Involved***
- **Various checks performed, Status Message provided, [redacted] server relays**

[redacted]

Additional Security Measures

System Roles

- Citizen
 - Have/will receive package [redacted]
 - Can register, vote, and check status
- [redacted] Local Admin
 - Allows [redacted] staff in [redacted] server location) to perform all [redacted] server activities
- [redacted] Remote Admin
 - Allows [redacted] staff [redacted] to access read-only features such as reports and event logs
- [redacted] Local Admin
 - Allows [redacted] staff to execute their duties on the [redacted] server and perform periodic system backup and audit log checks

[redacted]

Personnel Access Control

- Certificate-based access control for citizens
 - Portable Security - "Floppy is the Token"
 - Access limited to [redacted] participants
 - Access control based on Citizen's Common Name

- SSL3 Certificate-based access control for [redacted] admin staff
 - Admin staff authenticated using standard SSL3 mechanisms
 - Access limited to small list of authorized personnel
 - Access control based on Admin's Common Name

[redacted]

Transmission Security

- SSL3 without required client certificates between Citizens and the [redacted] Server
 - Citizen is NOT required to load certificate into the browser prior to accessing the system
- SSL3 with client authentication for [redacted] admin staff
 - Certificates must be installed into the browser prior to accessing the system
- SSL3 without required client certificates between [redacted] servers
 - COTS web products do not support certificate exchange for mutual authentication!

[redacted]

Transmission Security

- Router based security
 - Access control filters
 - Access restricted based on source and destination IP addresses
 - Access restricted based on network service type (TCP, ICMP)
 - Access restricted based on TCP application service ports
 - IPSec between [redacted] servers for access control
 - Provides redundant encryption with SSL3 transmission security
 - Provides strong two-way authentication between [redacted] server sites
 - Alleviates shortfalls of COTS web products!!!

[redacted]

Cryptographic Security Services

- Digital signatures (1024 bit keys) widely used for various security services
 - Authentication
 - Data integrity
 - Non-repudiation
- E-Ballot encryption (112 bit keys) modeled after S/MIME secure messaging model for confidentiality (secret ballot)
 - E-Ballots encrypted using [redacted] privacy certificate
 - Only authorized [redacted] staff can ever decrypt E-Ballots

[redacted]

EXHIBIT D

A two page document prepared subsequent to March 30, 2001, entitled "Project Assessment Report



Project Assessment Report

[redacted]. Booz·Allen & Hamilton did an outstanding job of assisting [redacted] in defining the concept for this pioneering effort, in designing and implementing an innovative system, and in assessing project results. [redacted]

The [redacted] volunteer citizens—a very special group of people—[redacted] realized the potential of this technology to make [redacted] voting more accessible and were willing to contribute their individual efforts to help make it happen.

Finally, I want to recognize the [redacted] development team for their extraordinary efforts in meeting all project objectives, including preserving the integrity of the electoral process, and ensuring that the [redacted] System was fielded on schedule for the November 2000 Presidential Election. All of these individuals have demonstrated that with a shared vision, a sense of urgency, and a focus on success, a vision can be realized.

Director

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.